OVERVIEW

Network-Centric Naval Forces

A Transition Strategy for Enhancing Operational Capabilities

NAVAL STUDIES BOARD

OVERVIEW

Network-Centric Naval Forces

A Transition Strategy for Enhancing Operational Capabilities

Committee on Network-Centric Naval Forces
Naval Studies Board
Commission on Physical Sciences, Mathematics, and Applications
National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C.

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This work was performed under Department of the Navy Contract N00014-96-D-0169/0001 issued by the Office of Naval Research under contract authority NR 201-124. However, the content does not necessarily reflect the position or the policy of the Department of the Navy or the government, and no official endorsement should be inferred.

Copies available from:

Naval Studies Board
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities, the full report from which this Overview is extracted, will be available from the Naval Studies Board at the address above.

Printed in the United States of America

THE NATIONAL ACADEMIES

National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

COMMITTEE ON NETWORK-CENTRIC NAVAL FORCES

VINCENT VITTO, Charles S. Draper Laboratory, Inc., *Chair*
ALAN BERMAN, Applied Research Laboratory, Pennsylvania State University
GREGORY R. BLACKBURN, Science Applications International Corporation
NORVAL L. BROOME, Mitre Corporation
JOHN D. CHRISTIE, Logistics Management Institute
JOHN A. CORDER, Colleyville, Texas
JOHN R. DAVIS, Center for Naval Analyses
PAUL K. DAVIS, RAND and RAND Graduate School of Policy Studies
JOHN F. EGAN, Nashua, New Hampshire
BRIG B. ELLIOTT, GTE Internetworking
EDWARD A. FEIGENBAUM, Stanford University
DAVID E. FROST, Frost and Associates
ROBERT H. GORMLEY, Oceanus Company
FRANK A. HORRIGAN, Raytheon Systems Company
RICHARD J. IVANETICH, Institute for Defense Analyses
WESLEY E. JORDAN, JR., Bolt, Beranek and Newman Co.
DAVID V. KALBAUGH, Applied Physics Laboratory, Johns Hopkins University
ANNETTE J. KRYGIEL, National Defense University
TERESA F. LUNT, Xerox Palo Alto Research Center
DOUGLAS R. MOOK, Sanders, a Lockheed Martin Company
DONALD L. NIELSON, Menlo Park, California
STEWART D. PERSONICK, Drexel University
JOSEPH B. REAGAN, Saratoga, California
CHARLES R. SAFFELL, JR., Titan Technologies and Information Systems Corporation
NILS R. SANDELL, JR., ALPHATECH, Inc.
WILLIAM D. SMITH, Fayetteville, Pennsylvania
MICHAEL G. SOVEREIGN, Monterey, California
H. GREGORY TORNATORE, Applied Physics Laboratory, Johns Hopkins University
PAUL K. VAN RIPER, Williamsburg, Virginia
BRUCE WALD, Center for Naval Analyses
RAYMOND M. WALSH, Basic Commerce and Industries, Inc.
MITZI M. WERTHEIM, Center for Naval Analyses
GEOFFREY A. WHITING, Sanders, a Lockheed Martin Company
DELL P. WILLIAMS III, Teledesic Corporation

Naval Studies Board Liaison

SEYMOUR J. DEITCHMAN, Chevy Chase, Maryland

Staff

RONALD D. TAYLOR, Director, Naval Studies Board
CHARLES F. DRAPER, Study Director
MARY G. GORDON, Information Officer
SUSAN G. CAMPBELL, Administrative Assistant
JAMES E. MACIEJEWSKI, Senior Project Assistant
SIDNEY G. REED, JR., Consultant
JAMES G. WILSON, Consultant

Navy Liaison Representatives

ROBERT LeFANDE, Associate Director, Systems Directorate, Naval Research Laboratory
CDR DAVID L. SPAIN, USN, Office of the Chief of Naval Operations, N513J (through July 1999)
CAPT(S) MARK TEMPESTILLI, USN, Office of the Chief of Naval Operations, N6C3

NAVAL STUDIES BOARD

VINCENT VITTO, Charles S. Draper Laboratory, Inc., *Chair*
JOSEPH B. REAGAN, Saratoga, California, *Vice Chair*
DAVID R. HEEBNER, McLean, Virginia, *Past Chair*
ALBERT J. BACIOCCO, JR., The Baciocco Group, Inc.
ARTHUR B. BAGGEROER, Massachusetts Institute of Technology
ALAN BERMAN, Applied Research Laboratory, Pennsylvania State University
NORMAN E. BETAQUE, Logistics Management Institute
JAMES P. BROOKS, Litton/Ingalls Shipbuilding, Inc.
NORVAL L. BROOME, Mitre Corporation
JOHN D. CHRISTIE, Logistics Management Institute
RUTH A. DAVID, Analytic Services, Inc.
PAUL K. DAVIS, RAND and RAND Graduate School of Policy Studies
SEYMOUR J. DEITCHMAN, Chevy Chase, Maryland, *Special Advisor*
DANIEL E. HASTINGS, Massachusetts Institute of Technology
FRANK A. HORRIGAN, Raytheon Systems Company
RICHARD J. IVANETICH, Institute for Defense Analyses
MIRIAM E. JOHN, Sandia National Laboratories
ANNETTE J. KRYGIEL, National Defense University
ROBERT B. OAKLEY, National Defense University
HARRISON SHULL, Monterey, California
JAMES M. SINNETT, The Boeing Company
WILLIAM D. SMITH, Fayetteville, Pennsylvania
PAUL K. VAN RIPER, Williamsburg, Virginia
VERENA S. VOMASTIC, The Aerospace Corporation
BRUCE WALD, Center for Naval Analyses
MITZI M. WERTHEIM, Center for Naval Analyses

Navy Liaison Representatives

RADM RAYMOND C. SMITH, USN, Office of the Chief of Naval Operations, N81
RADM PAUL G. GAFFNEY II, USN, Office of the Chief of Naval Operations, N91

Marine Corps Liaison Representative

LTGEN JOHN E. RHODES, USMC, Commanding General, Marine Corps Combat Development Command

RONALD D. TAYLOR, Director
CHARLES F. DRAPER, Senior Program Officer
MARY G. GORDON, Information Officer
SUSAN G. CAMPBELL, Administrative Assistant
JAMES E. MACIEJEWSKI, Senior Project Assistant

COMMISSION ON PHYSICAL SCIENCES, MATHEMATICS, AND APPLICATIONS

PETER M. BANKS, Veridian ERIM International, Inc., *Co-Chair*
W. CARL LINEBERGER, University of Colorado, *Co-Chair*
WILLIAM F. BALLHAUS, JR., Lockheed Martin Corporation
SHIRLEY CHIANG, University of California at Davis
MARSHALL H. COHEN, California Institute of Technology
RONALD G. DOUGLAS, Texas A&M University
SAMUEL H. FULLER, Analog Devices, Inc.
JERRY P. GOLLUB, Haverford College
MICHAEL F. GOODCHILD, University of California at Santa Barbara
MARTHA P. HAYNES, Cornell University
WESLEY T. HUNTRESS, JR., Carnegie Institution
CAROL M. JANTZEN, Westinghouse Savannah River Company
PAUL G. KAMINSKI, Technovation, Inc.
KENNETH H. KELLER, University of Minnesota
JOHN R. KREICK, Sanders, a Lockheed Martin Company (retired)
MARSHA I. LESTER, University of Pennsylvania
DUSA M. McDUFF, State University of New York at Stony Brook
JANET L. NORWOOD, Former U.S. Commissioner of Labor Statistics
M. ELISABETH PATÉ-CORNELL, Stanford University
NICHOLAS P. SAMIOS, Brookhaven National Laboratory
ROBERT J. SPINRAD, Xerox PARC (retired)

NORMAN METZGER, Executive Director (through July 1999)
MYRON F. UMAN, Acting Executive Director

Preface

The Chief of Naval Operations (CNO) recently declared that the Navy would be shifting its operational concept from one based on platform-centric warfare concepts to one based on network-centric warfare concepts. This new operational concept can be described as a model of warfare, called network-centric warfare, that derives its power from a geographically dispersed naval force embedded within an information network that links sensors, shooters, and command and control nodes to provide enhanced speed of decision making, rapid synchronization of the force as a whole to meet its desired objectives, and great economy of force.

Realization of a network-centric warfighting capability will depend on a number of factors: development of warfare concepts (and supporting doctrine) that determine how weapons, sensors, and information systems will interact to carry out specific missions; experimentation to test the viability of the new concepts; application of both military and commercial technology, particularly information technology, with essential attention to information and communications security and robustness; timely and effective acquisition of information technology assets; and education, training, and utilization of naval personnel to meet the demands of a network-centric force. This change of operational concept is also part of the Department of Defense (DOD) thrust toward Joint Vision 2010,[1] which encompasses efforts by the four Services to achieve similar objectives DOD-wide.

[1]Shalikashvili, GEN John M., USA. 1997. *Joint Vision 2010.* Joint Chiefs of Staff, The Pentagon, Washington, D.C.

Several initial steps have been taken by the Navy and Marine Corps toward achieving network-centric warfare capabilities. These include (1) promulgating the Navy Information Technology 21 (IT-21) initiative, which aims to bring the fleet up to date in information technology and related skills; (2) developing the Navy-Marine Corps intranet, to do the same for the shore establishment; (3) setting up the Navy Warfare Development Command and the Marine Corps Warfighting Laboratory, to develop concepts and doctrine; (4) testing these concepts and doctrines in fleet battle experiments and the Marine Corps "Warrior Series" experiments; and (5) making efforts toward interoperability of battle-group air defense and related command and control systems.

In a larger perspective, network-centric-type concepts have been applied by the Navy in the past, in antisubmarine warfare (ASW) since World War II, in approaches to air defense in the outer air battle in the 1980s, and more recently in the cooperative engagement capability (CEC) now under evaluation.

TERMS OF REFERENCE

At the request of Admiral Jay L. Johnson, USN, CNO (see Appendix A), the National Research Council (NRC), under the auspices of the Naval Studies Board (NSB), conducted a study to advise the Department of the Navy regarding its transition strategy to achieve a network-centric naval force through technology application. The terms of reference for the study call for an evaluation of the following:

- What are the technical underpinnings needed for a transition to network-centric forces and capabilities? Particular emphasis should be placed on assessing the means, the systems, and the feasibility of achieving and delivering data via links with the necessary bandwidth, capacity, and timeliness capabilities. Emphasis also should be placed on establishing and maintaining network security, emissions control when needed, and links with submarines, and on integrating information which may arrive intermittently and with different timescales.
- What near-term program actions need to be taken to begin the transition? What impact will these program actions have on the present platform-centric acquisition strategy? What impact will these program actions have on maintaining a robust industrial base to support the naval forces?
- Recognizing that many areas of technology are evolving faster than the naval forces can develop concepts for their use: What experimental programs need to be put in place to help the forces select needed technologies and systems, develop doctrine, and develop operational concepts that together can support the transition to a network-centric naval force? What organizational adaptations might facilitate rapid progress?
- What are the implications for both the business practices of the Department of the Navy and naval operations of moving away from a platform-centric

naval force to network-centric warfare? Implications for the following should be considered especially: resource priorities; force structure; personnel, education, career systems; warfighting doctrine; and coalition building and training with allies.

- Over what period of time can a transition strategy be implemented and in what details will the naval forces be different from today's forces when the strategy is finally implemented?
- What trends, if any, suggest that potential adversaries might move toward a network-centric military capability or exploit its vulnerabilities? What are the implications for U.S. naval forces?
- How will the move toward network-centric forces, if embraced by the Department of the Navy, be accomplished within the joint environment and subject to the likelihood of constrained future budgets?
- What are the implications of network-centric warfare for naval doctrine and for joint operations?

COMMITTEE'S APPROACH

In responding to the CNO's request, the committee organized itself into four ad hoc panels: (1) Panel 1—Concepts, Doctrine, Missions, and Operations; (2) Panel 2—System Architecture, Information Management, Dissemination, Protection, Assurance, and Command and Control; (3) Panel 3—Tactical Networks, Sensor-to-Shooter, Security, Protection, Targeting, Sensor Coordination, and Emission Control; and (4) Panel 4—Resources, Policy, Acquisition, Industrial Base, Career Issues, Education, and Training. In an effort to integrate the work of these four panels, an integration panel was formed with a lead representative from each panel, as well as the committee chair and NSB liaison.

The committee considered network-centric warfare, or better, network-centric operations (NCO), in the context of the Navy's principal missions—strategic deterrence, sea and air control, forward presence, and power projection. Because of its unique characteristics, strategic deterrence was not included in the study. Further, taking a mission-specific approach, the committee decided to focus on NCO in the power projection mission, since power projection must also encompass sea and air control (as well as a degree of forward presence), and, in anticipated littoral operations, the land-attack aspect of power projection was considered to be less developed with respect to NCO than sea and air control, with which the Navy has considerable experience.

The following report attempts to treat in as much detail as was feasible the issues raised in the terms of reference listed above. As often happens, once the study's directions of inquiry developed and results began to emerge, the committee found that its discussions of the issues raised in the terms of reference tended to group in a contextual and logical order different from the order initially antici-

pated. The next few paragraphs therefore sketch briefly where in the report discussions of the issues may be found.

The technical underpinnings needed for the transition to network-centric forces, capabilities, and operations are treated in detail throughout the report. Implications for naval force doctrine and joint operations are reviewed, directly and indirectly, in Chapters 1 and 2, while implications for joint operations in designing and creating NCO systems, in designing and creating a common information infrastructure (i.e., the Naval Command and Information Infrastructure, the NCII), and in undertaking network-centric combat operations are treated in detail at many points in Chapters 3, 4, 5, and 6 in connection with the overall topics of those chapters.

Presented in the Executive Summary is a short list of recommended near-term program, management process, and organizational actions that must be undertaken to begin the transition from platform-centric to network-centric naval forces. The list was developed from the more detailed sets of recommendations given in Chapter 1, which were, in turn, taken from the fully developed findings and recommendations in the body of the report.

The implications for Department of the Navy business practices and organizational responsibilities needed to better transition to network-centric operations are considered in detail in Chapter 7. Management and technical aspects of some business practices and acquisition strategy are covered further in parts of Chapters 2, 4, 5, and 6 in discussions of the need for a new approach to thinking about the naval forces under the NCO concept and in descriptions of the many aspects of NCII design, operation, and information assurance. Needed experimental programs are described as part of these discussions, in Chapter 2 and also in Chapter 3, in connection with the technical details of subsystems and components needed to complete the NCO orientation of the naval force systems.

The committee believes that NCO will rely on a dual industrial base. The purely military aspects of such systems will draw on the base that currently furnishes the platforms and the specialized sensors and weapons that will enter NCO subsystems and components. Much commercial off-the-shelf technology will also support these subsystems and components. The NCII will draw largely from the huge commercial technology base that is developing to support civilian communication and computer-based information networks (e.g., the Internet) and the exponentially increasing commercial activity that their presence is fostering. This commercial base is as much a driver of the U.S. military's movement to network-centric forces and warfare as it is an enabler for that movement.

The committee did not fully examine the capability of allies and potential coalition partners in the information and networking technology and systems areas relevant to network-centric operations. Similarly, it was not possible to investigate in depth, from the intelligence viewpoint, the possibility that potential adversaries could engage in network-centric conflict as defined in this report. The United States is so rapidly outpacing every other significant power in the

world in the area of linking military forces in large, computer-based information networks that it is difficult for intelligence to estimate where the rest of the world stands relative to the United States in this area.

This does not mean that U.S. network-centric operations capability is now or will in the future be safe from attack or interference. As detailed in Chapter 5, U.S. information and combat networks and the NCII have, because of their inherent design and by virtue of their reliance on the commercial technology base, many vulnerabilities. Anyone with modern computing and communications capability can wage information war or cyber war against the United States, often in ways that have no easy counter. Approaches to mitigating this risk are discussed in detail in Chapter 5.

Overall, the committee believes that it has assembled a relatively complete picture of the significance of the movement toward NCO for the naval forces in the joint environment. The menu of needed actions to achieve the capability is large and will require a dedicated and extended effort throughout the Department of the Navy, building on and greatly extending actions currently under way.

COMMITTEE MEETINGS

The committee first convened early in 1999 and met for approximately 8 months. During that time, it held the following committee and panel meetings:

- January 26-28, 1999, in Washington, D.C (Plenary). Organizational meeting. Navy, Marine Corps, Joint Chiefs of Staff, and Defense Advanced Research Projects Agency (DARPA) briefings on network-centric warfare.
- February 16-17, 1999, in Washington, D.C. (Representatives, Panels 1 and 3). Office of the Chief of Naval Operations concepts of operations and tactical data links briefings.
- February 18, 1999, in Washington, D.C. (Integration Panel).
- March 4-5, 1999, in Washington, D.C. (Panel 2). Defense Information Systems Agency (DISA), DARPA, Joint Chiefs of Staff, and Office of the Secretary of Defense information infrastructure and interoperability briefings.
- March 9 and 11, 1999, in Washington, D.C. (Panel 4). Joint Requirements Oversight Council, Navy, and Marine Corps assessment and requirements briefings.
- March 23, 1999, in Washington, D.C. (Plenary). Air Force Battlespace Infosphere, Army Digital Battlefield, Defense Science Board Integrated Information Infrastructure, and DARPA Discover II briefings.
- March 24, 1999, in Washington, D.C. (Representatives, Panels 1 through 4). DARPA, DISA, Military Satellite Communications Joint Program Office, and National Imagery and Mapping Agency information dissemination and management briefings. Naval Air Systems Command weapons, Navy Warfare Devel-

opment Command concepts of operations, and Office of the Secretary of Defense acquisition and technology briefings.

- March 25, 1999, in Washington, D.C. (Integration Panel).
- April 15-16, 1999, in Washington, D.C. (Panel 2). CitiGroup, DARPA, Naval Research Laboratory, and Office of Naval Research information assurance and security briefings.
- April 19, 1999, in Alexandria, Virginia (Representatives, Panels 2 and 3). National Reconnaissance Office briefings.
- April 20-21, 1999, in Washington, D.C. (Representatives, Panels 1, 3, and 4). Office of the Secretary of Defense and Marine Corps C4ISR requirements briefings. Air Force Rivet Joint and U2 briefings.
- April 27-29, 1999, in San Diego, California (Panel 2). Site visit to Space and Naval Warfare Systems Command. Briefings on information assurance and infrastructure programs, as well as related network-centric topics.
- May 19-20, 1999, in Washington, D.C. (Representatives, Panels 1 through 4). Air Force Expeditionary Force Experiment, DARPA information assurance, Joint Theater Air and Missile Defense Organization single integrated air picture, naval intelligence threat, and Naval Sea Systems Command battle force interoperability requirements briefings.
- May 21, 1999, in Washington, D.C. (Integration Panel).
- June 8-9, 1999, in Crystal City, Virginia (Panel 4). Navy and Air Force briefings on DD-21 and Joint Strike Fighter, respectively.
- June 16-17, 1999, in Washington, D.C. (Panel 2).
- June 21, 1999, in Washington, D.C. (Panel 4).
- June 23, 1999, in Washington, D.C. (Panel 1).
- June 22-23, 1999, in Washington, D.C. (Panel 3).
- June 24, 1999, in Washington, D.C. (Plenary). Status from panels.
- June 25, 1999, in Washington, D.C. (Integration Panel).
- July 13-14, 1999, in Washington, D.C. (Panel 4).
- July 19-23, 1999, in Woods Hole, Massachusetts (Plenary).
- August 31 to September 1, 1999, in Washington, D.C. (Integration Panel).
- September 29 to October 1, 1999, in Washington, D.C. (Integration Panel).
- November 8-10, 1999, in Washington, D.C. (Integration Panel).
- January 11-12, 2000, in Washington, D.C. (Integration Panel).

Acknowledgments

The Committee on Network-Centric Naval Forces extends its gratitude to the many individuals who provided valuable information and support during the course of this study. Special acknowledgment goes to VADM Arthur K. Cebrowski, USN, president, Naval War Colleges, who formulated the concept of network-centric warfare. His knowledge and insights made an invaluable contribution to the success of the study.

The committee extends a special thanks to the Navy liaisons to the committee, CAPT(S) Mark Tempestilli, USN, CDR David Spain, USN, and Dr. Robert LeFande, who responded to the committee's numerous requests for information throughout the stages of the study.

The committee also thanks Mr. Kin Searcy, who helped arrange a visit to the Space and Naval Warfare Systems Command. He and his staff were gracious in hosting members of the committee on its 4-day site visit to learn more about ongoing Navy information technology investments.

In addition, the committee wishes to thank Mr. Paul Blatch, who serves as the Navy's action officer for Naval Studies Board activities and assisted with this study from its inception to completion.

The committee is grateful to the staff of the Naval Studies Board for its assistance, support, and guidance throughout the course of the study and especially to Ms. Susan Maurizi for editing the manuscript.

Finally, the committee thanks the many men and women throughout the Armed Services, as well as government, academic, and industry leaders who provided the committee with insightful discussions throughout the course of this study. Without their combined efforts, the committee's report would not have been possible.

Acknowledgment of Reviewers

This report has been reviewed by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the authors and the NRC in making the published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The contents of the review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. The committee wishes to thank the following individuals for their participation in the review of this report:

William F. Ballhaus, Jr., Lockheed Martin Corporation,
Ruth M. Davis, Pymatuning Group, Incorporated,
John S. Foster, Jr., TRW, Incorporated,
Robert A. Frosch, Harvard University,
Charles M. Herzfeld, Silver Spring, Maryland,
Anita K. Jones, University of Virginia,
David A. Richwine, Fairfax, Virginia,
John P. Stenbit, TRW, Incorporated,
Jerry O. Tuttle, ManTech Systems Engineering Corporation,
Andrew J. Viterbi, QUALCOMM, Incorporated, and
Larry Welch, Institute for Defense Analyses.

Although the individuals listed above provided many constructive comments and suggestions, responsibility for the final content of this report rests solely with the authoring committee and the NRC.

Contents

Executive Summary

ES.1 WHAT ARE NETWORK-CENTRIC NAVAL FORCES?

ES.1.1 Network-Centric Operations Defined

This report responds to a request from the Chief of Naval Operations to help the Navy "[realize] . . . the full potential of network-centric warfare. . . ."[1] The committee received many briefings on the subject, none of which defined "network-centric warfare" in the same way. Thus, the committee deemed it important to establish a common basis of understanding regarding what is meant by the "network centric" concept and its characteristics within the Department of the Navy and from there into the joint arena. Further, it concluded that once adopted as an organizing principle the concept must apply to *all* military force operations, in peace as well as in war. The committee therefore defined network-centric operations (NCO) as *military operations that exploit state-of-the-art information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness.*

ES.1.2 The Promise and Significance of Network-Centric Operations

In network-centric operations naval force assets are linked together to carry out a mission in ways that were not previously possible, through the application of modern means of acquiring, processing, disseminating, and using information

[1]See Appendix A.

and information networks. The gathering, exploitation, and transmission of information about the enemy and the environment have always been of critical importance in guiding military operations. The means for doing so have become so powerful in recent times that they have overtaken the capabilities of individual platforms and weapons as primary drivers of global naval force capability.

Network-centric operations thus represent a new force design and operational paradigm for the naval forces. In network-centric operations, naval force and other Service elements, organized as a single, joint, networked system, will be able to achieve mission objectives far more rapidly, decisively, and with greater economy of force than was possible earlier. However, the entire, joint system will be more intricate than any the naval forces and joint forces have ever dealt with in the past. For the Navy and the Marine Corps, the transition to NCO will require that many of the traditional approaches to development and operations be transformed into new methods and concepts of operation.

ES.1.3 Attributes of Naval Forces in Network-Centric Operations

The key attribute of NCO is the unprecedented ability to support well-informed and rapid decision making by naval force commanders at all levels, within a system of flexible and adaptable command relationships. The information network and infrastructure in which the naval force elements will be embedded will enable dynamic adjustment and adaptation to battlespace situations and needs as they emerge. Multiple platforms separated by great distances will be able to work as closed-loop systems with the same speed and assurance that have characterized single platform-weapon combinations. Within the physical limits of time required for movement and weapon range and speed, the force commanders operating in the network-centric mode will be able to concentrate widely dispersed forces' fire and maneuvers at decisive locations and times. The forces will be able to achieve the precision needed to identify and engage opposing forces and specific targets with minimal casualties and the least civilian damage. And they will be able to do so at a pace that overwhelms the opposition's ability to prevent the actions or to respond in time to avoid defeat.

To develop these attributes of NCO, information and networking technology will have to be applied to achieve the following, to the greatest extent possible:

- Knowledge of where all U.S., allied, neutral, and opposition installations, forces, and platforms are, in terms of common space and time coordinates, in time to use the knowledge to desired military effect;
- Sharing of processed information throughout the force as and when needed by the decision makers at various command levels;
- Coordination of all (possibly widely dispersed) assets—sensors, weapons, platforms, Marine units—to operate as a common whole; and

• Assurance that the information that is gathered and distributed is timely, accurate, and not subject to disruption, corruption, or exploitation by the opposition.

ES.1.4 The Inevitability of Network-Centric Operations

The committee believes that development of the naval forces in the direction of network-centric operations is inevitable, because of both the push of developing threats worldwide and the pull of opportunities that the information and networking technology offers.

All of the following are becoming available to potential opponents of U.S. naval forces: stealth in antiship missiles; quieter submarines; long-range air defenses with counterstealth characteristics; battlefield ballistic missiles that may have chemical, biological, and eventually nuclear warheads; hiding of organized criminal, terrorist, and irregular forces in civilian populations and difficult terrain; cell phone and satellite communication and navigation; and cyber-warfare capability. A concatenation of such threats can be met only by sharing, among all friendly force elements, information gathered by widely dispersed assets and fused to make a coherent operational and tactical picture for the force's decision makers, so as to enable an effective response or preemptive action, all in less time than it takes the threat to strike. Information and networking technology makes such sharing possible.

In addition, current and, it is expected, future U.S. superiority in exploiting the technology presents the opportunity to build naval forces that will be able to undertake the decisive operations basic to success in missions as far into the future as can be foreseen.

ES.2 TRANSITION TO NETWORK-CENTRIC NAVAL FORCES

To achieve naval forces able to perform as described will require leadership from the top levels of the Navy Department; new concepts of operation; a common information infrastructure with assured reliability and integrity of the information that passes through it; and an integrated approach to shaping the Navy and the naval forces.

ES.2.1 Leadership

The Department of the Navy's top leadership must convey understanding, acceptance, and their continuing support of the concept of network-centric operations throughout the naval forces, including their anticipation of and support for the NCO-induced changes in command relationships that will inevitably come about as the command and information structure of the naval forces evolves.

Recommendation 1: The Secretary of the Navy, the Chief of Naval Operations (CNO), and the Commandant of the Marine Corps (CMC) should agree on the basic concepts essential to transforming today's naval forces to network-centric forces, including:

a. Integrating all the naval force elements involved in a mission into an adaptive, comprehensive, information-driven NCO system;

b. Adopting the spiral development process that is described in this report[2] as the primary development and procurement mechanism for creating such NCO systems;

c. Constructing a common command and information infrastructure (the Naval Command and Information Infrastructure; NCII[3]) as the framework that enables the creation and effective utilization of effective NCO systems; and

d. Making the attending adjustments and enhancements in organization and management.[4]

They should promulgate those concepts throughout the naval forces as top-level policy.

ES.2.2 Concepts of Operation

Operations in which all force elements are closely coupled and function as a single system within a common command and information network will differ in speed and character of execution from those familiar in the past. New kinds of operations will be possible, as illustrated by the recent development of the cooperative engagement capability for fleet air defense. The flow of information from many sources to multiple command levels will tend to flatten the combat command hierarchy within agreed mission plans and rules of engagement. All future military operations, in peace and in war, will be joint, and will occur most often in coalitions. Even when the Navy and Marine Corps are the only military forces at a point of action, the information network and the sensors that the forces rely on will be interconnected with information assets from other Services and National[5] agencies. Command and information links with coalition partners will also have to be assured.

The CNO and the CMC have assigned to the Navy Warfare Development Command (NWDC) and the Marine Corps Combat Development Command (MCCDC), respectively, the responsibility for developing new concepts of operation in the joint and combined environment. Each of these organizations is

[2]See Chapters 1 and 2.

[3]See Chapters 1, 4, and 6.

[4]See Chapters 1 and 7.

[5]The term "National" refers to those systems, resources, and assets controlled by the U.S. government, but not limited to the Department of Defense.

devising concepts for its parent Service. However, the naval forces as a whole cannot function in the NCO mode unless they share common concepts of operation involving both Services.

Recommendation 2: The CNO and the CMC should assign NWDC and MCCDC the responsibility to work *together* to devise joint concepts and doctrine for network-centric operations of the naval forces as a whole. Joint and coalition aspects of such operations should be incorporated in the concepts developed.

ES.2.3 Common Command and Information Infrastructure

Network-centric operations require an infrastructure that supports not only the manipulation and transport of information but also the actual functions of command, to hold the elements of the network together and guide their operation in concert as an integrated system according to the NCO concept. That infrastructure, the NCII, will include the communications trunk lines, the terminals, the central processing facilities, the common support applications, connectivity to tactical networks, and the Department of Defense (DOD)-wide and commercial standards, rules, and procedures that will enable the flow of raw and processed information and commands at all levels of command among units that are involved in an action. The NCII will be connected to, and will essentially have to become a part of, the joint National and coalition information infrastructures to the extent that all will function as a single infrastructure to ensure consistency and interoperability among all the parts.

Recommendation 3: The Secretary of the Navy, the CNO, and the CMC should arrange for assembly, augmentation, and interweaving of all related ongoing efforts[6] to begin creating the NCII as a common command and information infrastructure to provide the global framework for networked naval force operations.

Recommendation 4: The Secretary of the Navy, the CNO, and the CMC should develop a comprehensive and balanced transition plan to aid realization of the functional capabilities necessary for the NCII (as described in the detailed recommendations in the body of this report[7]).

---

[6]As discussed at length in Chapters 4 and 6, these efforts include the Navy's IT-21 strategy, the Global Command and Control System–Maritime, common-user long-haul communications, tactical networks, common support application software, and sensor and intelligence feeds, including as necessary other joint and National assets.

[7]See Chapter 6.

ES.2.4 Information Assurance

Many threats[8] will arise from the very structure of the NCII, and also from the need to rely heavily on civilian systems for the transport of data and processed information, the need to share information and techniques with coalition partners, and the potential for damaging actions by malicious insiders who may also be enemy agents. There is currently no single individual within the Department of the Navy who has the responsibility and authority to ensure the integrity of the NCII and the information that flows through it, and the timeliness and continuity of the information flow.

Recommendation 5: The Secretary of the Navy, the CNO, and the CMC should assign responsibility for information assurance at a high enough level within the Navy and the Marine Corps, and with sufficient emphasis, to ensure that adequate and integrated attention is paid to all aspects of information assurance in the design and operation of the NCII.

Recommendation 6: The CNO and the CMC should take steps to ensure that fleet and Marine training encompasses situations with impaired information and NCII functionality, and that fallback positions and capabilities are prepared to meet such eventualities.

ES.2.5 Integrated Approach to Shaping the Navy and the Naval Forces

Network-centric operations will span all Navy and Marine Corps activities. Since the force components, the people in the force, and the information network in which they are embedded will be treated as a complete system, the new approach to shaping the Navy and the naval forces will entail performance and economic trade-offs among *all* the parts of the system—weapons, platforms, people, command, control, and information assets—not simply *within* the parts as has been customary heretofore. And there will have to be corresponding organizational and business practice adjustments in the Navy and the naval forces to suit the new conditions. The committee examined alternative approaches to achieving these changes but concluded that the best Department of the Navy strategy to meet these needs would be to build on existing organizations with some changes in emphasis.

The following needs were identified, and recommended approaches to meeting these needs are given. It is, of course, recognized that internal and external considerations that were not known to the committee may lead the Navy Department to reach other solutions to the problems posed.

[8]Described in detail in Chapter 5.

• In the current fleet/Office of the Chief of Naval Operations (OPNAV)/ Systems Command (SYSCOM) organizational relationships, there is no mechanism for integrating cross-platform/cross-mission needs of the battle force in operations information—including terrestrial and space assets; command, control, communication, computing, intelligence, surveillance, and reconnaissance (C4ISR); and the NCII. The lack of a type commander[9] resource for C4I who can interact with the platform type commanders exacerbates this cross-platform integration problem.

Recommendation 7: The Secretary of the Navy and the CNO should create a new functional type commander, the Commander for Operations Information and Space Command, to be the single point of information support to all the fleets. Responsibilities for the new functional type commander and related other changes in Navy organizational responsibilities are described in the detailed recommendations in the body of this report.[10]

• A mechanism is needed to integrate various competing and complementary requirements presented by the fleets to ensure rapid improvement of at-sea operational capabilities in the NCO mode through the spiral development process.

Recommendation 8: The CNO should establish a requirements board [11] under the chairmanship of the Vice Chief of Naval Operations to deal with operations information and to integrate requirements presented by the fleets as the NCII is assembled and other NCO plans and acquisitions take shape.

• An authority is needed to make funding, scheduling, and program adjustments, trade-offs, and decisions in relevant areas, based on review, oversight, and prioritization of the acquisition, installation, and program execution aspects of NCO systems treated in an integrated fashion.

Recommendation 9: The Secretary of the Navy, the CNO, and the CMC should establish a board of directors[12] under the chairmanship of the Undersecretary of the Navy to provide coordinated guidance and ensure the integration and interoperability of all the Navy and Marine Corps NCO acquisition and program execution activities.

• Decision support and program execution mechanisms are needed to improve and enhance implementation of the decisions made by the above authority.

---

[9]The flag officer who has responsibility for all ships of a certain type in the fleet.
[10]See Chapters 1 and 7.
[11]See Chapters 1 and 7.
[12]See Chapters 1 and 7.

Recommendation 10: The CNO should strengthen mission analysis and component trade-off evaluations by (1) providing staff and resources for the integrated warfare architecture (IWAR) process to enable continuous assessments from requirements generation through programming, budgeting, and execution; (2) developing output-oriented measures of effectiveness and measures of performance for network-centric operations; and (3) developing a comprehensive set of design reference missions across all missions areas. Resource planning should support the spiral development process.

a. The Secretary of the Navy and the CNO should appoint a designated SYSCOM Commander to be a deputy to the Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN (RDA)) for Navy NCO integration.

b. The Secretary of the Navy should adjust the responsibilities of the Chief Information Officer, the Chief Engineer, and the N6, with due account for authorities and responsibilities established in law, to enable the implementation and operation of the NCII, including interaction and collaboration with the other Services, the joint community, and defense agencies.[13]

- There is a need to ensure that all missions are given balanced emphasis in the naval force planning and acquisition processes. In particular, the committee found that the power projection mission is not as well represented in the planning process as other naval force missions. Special attention is needed to the planning and design of end-to-end (surveillance and targeting through effectiveness assessment) fleet-based land-attack (strike and fire support) subsystems for network-centric operations.[14]

Recommendation 11:

a. The ASN (RDA) and the CNO should review the Navy's overall planning and acquisition processes and if necessary and as appropriate adjust the program executive office structure to orient it toward the integrated design and acquisition of systems suited to network-centric operations.

b. The CNO should review and if necessary and as appropriate adjust the N8 structure and assignments within his staff to ensure balanced attention to all missions, including the mission of power projection from the sea.

- Without effective, appropriately educated and trained people the NCO concept cannot be made to work. To be fully effective in implementation over

[13]See Chapters 1, 4, and 7.

[14]See Chapters 1, 3, and 7. There were some differing views within the committee regarding the following recommendations, as indicated in related discussion in these chapters.

the long term, NCO concepts must pervade the Navy and Marine Corps training and education system. This approach includes identifying the qualifications for billets critical to network-centric operations (including both domain and infrastructure experts); identifying training and education needs for those billets; developing career paths for both military personnel and civil service employees to retain and reward those with information technology expertise; and orienting the education of naval officers toward NCO concepts from the beginning of their schooling.[15]

Recommendation 12: The CNO and the CMC should review NCO education and training at all levels across the Navy and the Marine Corps, and institute changes as necessary and appropriate to achieve the objectives outlined above.

- Research and development is needed to meet the challenges of creating an advanced NCII, including providing for information assurance, and to meet the new challenges of network-centric operations, including especially support of the power projection mission in NCO.

Recommendation 13: The ASN (RDA), the CNO, and the CMC should join with the other components of DOD to sponsor a vigorous, continuing research and development program aimed at the objectives noted above.

The above recommendations, and related ones, are expanded and discussed more fully in the overview that follows this summary. Many additional recommendations for actions to reorient the naval forces toward NCO, involving many areas of naval force endeavor, emerged from this study. All the recommendations, including those above and many others, are developed in detail and presented in the main body of the report.

[15]See Chapters 1 and 7.

1

Overview of Study Results

1.1 MISSION EFFECTIVENESS: WHAT IS REQUIRED

1.1.1 Joint Vision 2010

In one way or another all military operations will be joint. That is, systems and forces from all the Services and from National agencies will contribute to the U.S. Armed Forces' operations in ways that vary with the circumstances. Developed in the past few years by the Joint Chiefs of Staff, Joint Vision 2010[1] envisions how the Armed Forces will channel the vitality and innovation of the nation's people and use the leverage offered by advancing technology to achieve unprecedented levels of power, timeliness, and decisiveness in joint operations and warfighting. The Navy and Marine Corps have also developed conceptual descriptions of their own future warfighting strategies—"Forward...From the Sea"[2] and "Operational Maneuver From the Sea"[3]—that have themes in common with Joint Vision 2010. Most importantly, all of these concepts have recog-

[1]Shalikashvili, GEN John M., USA. 1997. *Joint Vision 2010,* Joint Chiefs of Staff, The Pentagon, Washington, D.C.

[2]Department of the Navy. 1997. "Forward...From the Sea," U.S. Government Printing Office, Washington, D.C.

[3]Headquarters, U.S. Marine Corps. 1996. "Operational Maneuver From the Sea," U.S. Government Printing Office, Washington, D.C., January 4.

nized the fundamental role that information superiority will play in the forces' ability to prevail over adversaries.[4]

Focusing on achieving dominance across the range of military operations through the application of new operational concepts, Joint Vision 2010 provides a joint framework of doctrine and programs within which the Services can develop their unique capabilities as they prepare to meet an uncertain and challenging future. The scope and complexity of the challenges and the capabilities required to meet them were projected in a recent Naval Studies Board report (the TFNF—Technology for Future Naval Forces—study;[5] see Box 1.1), an effort from which this current study follows naturally.

1.1.2 Network-Centric Operations

The implications of Joint Vision 2010, future naval operational concepts, and the spread of advanced technology and commercial information systems worldwide make it inevitable that joint forces, and particularly forward-deployed naval forces, must move toward network-centric operations. The committee defines such operations as follows: *Network-centric operations (NCO) are military operations that exploit state-of-the-art information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness.*

Forward deployment of naval forces that may be widely dispersed geographically, the use of fire and forces massed rapidly from great distances at decisive locations and times, and the dispersed, highly mobile operations of Marine Corps units are examples of future tasks that will place significant demands on networked forces and information superiority. Future naval forces must be supported by a shared, consolidated picture of the situation, distributed collaborative planning, and battle-space control capabilities. In addition, the forces must be capable of coordinating and massing for land attacks and of employing multisensor networking and targeting for undersea warfare and missile defense.

In network-centric operations, the supporting information infrastructure, ideally, will deliver the right information to the right place at the right time to achieve the force objectives. Also, although rules of engagement (ROEs) are

[4]*Joint Vision 2010* (p. 16) defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Information superiority will therefore require "both offensive and defensive information warfare" capabilities.

[5]Naval Studies Board, National Research Council. 1997. *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force,* 9 volumes, National Academy Press, Washington, D.C.

usually determined politically and morally, accurate information delivered rapidly to a commander may affect how ROEs are applied, for example, by providing input to decisions for preemptive attack in primarily defensive situations. Network-centric operations must also ensure that when forces move and weapons are delivered according to the information furnished, they arrive at the right places and times to achieve the force objectives. Thus, the command relationships, the information systems and networks, implementations of ROEs, and the combat forces themselves must all evolve toward network-centric operations together.

The trend toward network-centric operations is inevitable. There are many reasons why this is so. One reason is the pull of opportunity: The anticipated effectiveness of joint, networked forces is compelling. A second is the push of necessity: Threats are becoming more diverse, subtle, and capable. If they are to be discerned, fathomed, and effectively countered in timely fashion, increasingly complex information gathering and exploitation will be required. Also, the diversity and geographic spread of potential threats and operations, many of which will occur simultaneously or nearly so, demand that forces of any size be used to their maximum effectiveness and efficiency. Another reason derives from the relentless advance of U.S. and foreign technology in both the civilian and military spheres: There will be no other way for U.S. forces to develop. Only a force that is attuned to and capable of harnessing the power of the information technology that drives modern society will be able to operate effectively to protect that society.

The naval forces are already moving toward network-centric operations. Joint task force commands afloat are being established to direct ongoing operations and are the subjects of fleet battle experiments. Elements of network-centric forces and operations are both in place and in the making, in the Aegis system and its extensions to theater missile defense, and in the cooperative engagement capability (CEC) for fleet defense against cruise missiles and its shoreward extensions.[6] The Navy's information technology thrust is becoming

[6]It is remarkable that in World War II the U.S. Navy's Tenth Fleet exercised network-centric antisubmarine warfare (ASW) operations in the Battle of the Atlantic against German submarines, characterized by Morison as ". . . a contest between systems of information . . ." (as quoted by Cohen, Eliot A., and John Gooch. 1990. *Military Misfortunes; The Anatomy of Failure in War,* The Free Press, A Division of Macmillan, Inc., New York and Collier Macmillan Publishers, London, p. 75). The Tenth Fleet integrated information from distant direction-finding fixes with data from local high-frequency direction finder and radar contact from forces in the action area with decrypted messages and other intelligence from vessels attacked, and with the help of a strong operational analysis group directed the coordinated efforts of warships, aircraft, and convoy commanders, with time delays from initial detection to action orders of minutes to hours. The Tenth Fleet also shared its operational picture and coordinated actions with the British in charge of the Eastern Atlantic ASW operations and conducted information warfare in the form of psychological warfare messages directed specifically to the enemy submarines at sea.

Box 1.1 Future Naval Operations

Technology for the United States Navy and Marines Corps, 2000-2035 (the TFNF study)[1] projected that future naval forces would continue to be required to perform tasks such as the following (Vol. 1, *Overview*, p. 3):

- Sustaining a forward presence;
- Establishing and maintaining blockades;
- Deterring and defeating attacks on the United States, our allies, and friendly nations, and, in particular, sustaining a sea-based nuclear deterrent force;
- Projecting national military power through modern expeditionary warfare, including attacking land targets from the sea, landing forces ashore and providing fire and logistic support for them, and engaging in sustained combat when necessary;
- Ensuring global freedom of the seas, airspace, and space; and
- Operating in joint and combined settings in all these missions.

These tasks are not new for the naval forces and have changed little over the decades. However, advanced technology is now spreading around the world, and burgeoning military capabilities elsewhere will, in hostile hands, pose threats to U.S. naval force operations. The most serious are as follows (pp. 4-5):

- Access to and exploitation of space-based observation to track the surface fleet, making surprise more difficult to achieve and heightening the fleet's vulnerability;
- Increased ability to disrupt and exploit technically based intelligence and information systems;
- Effective antiaircraft weapons and systems;
- All manner of mines, including "smart" minefields with networked sensors that can target individual ships for damage or destruction by mobile mines;
- Antiship cruise missiles with challenging physical and flight characteristics;
- Accurately guided ballistic missiles able to attack the fleet;
- Quiet, modern, air-independent submarines with modern torpedoes; and
- Nuclear, chemical, and biological weapons.

Future naval forces must be designed to meet these threats while maintaining the forward presence and operational flexibility that have characterized U.S. naval forces throughout history. This capability must be achieved in a world of ever advancing technology (particularly information technology) available globally through the commercial sector and sales to foreign military users.

The TFNF study described the characteristics of future naval force operations as follows (p. 6):

- Operations from forward deployment, with a few major, secure bases of prepositioned equipment and supplies;
- Great economy of force based on early, reliable intelligence; on the timely acquisition, processing, and dissemination of local, conflict-, and environment-related information; and on all aspects of information warfare;
- Combined arms operations from dispersed positions, using stealth, surprise, speed, and precision in identifying targets and attacking opponents, with fire and forces massed rapidly from great distances at decisive locations and times;

- Defensive combat operations and systems, from ship self-defense through air defense, antisubmarine warfare, and antitactical ballistic missile defense, always networked in cooperative engagement modes that extend from the fleet to cover troops and installations ashore;
- Marine Corps operations in dispersed, highly mobile units from farther out at sea to deeper inland over a broader front, with more rapid conquest or neutralization of hostile populated areas, in the mode currently evolving into the doctrine for Operational Maneuver From the Sea;
- Extensive use of commercial firms for maintenance and support functions; and
- Extensive task sharing and mission integration in the joint and combined environment, with many key systems, especially in the information area, jointly operated.

The TFNF study concluded that these future threats and operational requirements would demand the development of new naval force capabilities, which would in turn necessitate a complete transformation of future naval forces. These breakthrough capabilities included the following (p. 5):

- Sustained information superiority over adversaries;
- Major ships operated effectively by fewer people, through the use of networked instrumentation and automated subsystems [with high maintainability and reliability];
- A family of rocket-propelled, guided missiles, significantly lower in cost than today's weapons, that will greatly increase the responsiveness, rate of fire, volume of fire, and accuracy of strike, interdiction, and supporting fire from surface combatants and submarines;
- STOL [short takeoff and landing] or STOVL [short takeoff and vertical landing], stealth, and standoff in combat aircraft;
- Cooperative air-to-air engagement at long range using networked multistatic sensor, aircraft, and missile systems;
- Use of unmanned aerial vehicles (UAVs) for both routine and excessively dangerous tasks;
- Greatly expanded submarine capability to support naval force operations ashore;
- Recapture of the antisubmarine warfare advantage that has been eroded by quieting of Russian nuclear submarines and by advanced air-independent nonnuclear submarines that are being sold by other nations on world markets;
- The ability to negate minefields at sea, in the surf, and on the beaches much more rapidly than has been possible heretofore;
- Novel weapons, systems, and techniques for fighting in populated areas, against organized military forces, irregulars, and terrorist and criminal groups; and
- Logistic support extensively based at sea that will provide needed materiel on time with far less excess supply in the system than has been the case in the past.

---

[1]Naval Studies Board, National Research Council. 1997. *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force*, 9 volumes, National Academy Press, Washington, D.C.

evident in the fleet and its support operations. During the Cold War, networked antisubmarine warfare (ASW) systems were devised to overcome the Soviet submarine threat. As the TFNF report points out, networked operations will become necessary to achieve an effective defense against quiet submarines in the littoral environment and against mine warfare; effective fleet fire and logistic support of Marines ashore in Operational Maneuver From the Sea (OMFTS); and effective protection against growing air defense capabilities of potential adversaries that will demand engagements at very long ranges.

Today, however, all of these network-centric operations and capabilities, existing and under development, are evolving in an essentially fragmented and stand-alone manner. The focus is still on the subsystems or components of the total naval force combat system, and they are not yet fully coordinated with one another. It has become clear that unless networked naval forces are treated as a total system, a great deal of money will be wasted and opportunities to enhance warfighting capabilities will be lost. Beyond optimizing individual sensors, weapons, and command, control, communications, and intelligence (C3I) systems, it is essential to achieve overall optimization of the total system of networked combat assets, including the information that ties them all together and makes them fully effective.

Network-centric operations with fully networked forces will provide the significant advances demanded for success in future warfighting and in countering the capabilities of future adversaries. They will enable better and faster battlespace decisions, providing time and direction for rapid, integrated execution of tasks with flexible use of both dispersed and concentrated (and other joint and combined) assets. At the same time, however, network-centric operations will present significant new vulnerabilities that must be actively managed through the application of technology and doctrine. Both aspects of network-centric operations are treated in this report.

1.1.3 Approach and Emphasis in This Report

This report describes the operational concepts, command and control relationships, and information systems architecture necessary to support the networked naval forces. Many requirements for sensor and weapon systems assets in the future systems are also discussed, as is information assurance, which is critical to achieving true information superiority.

In keeping with the definition of network-centric operations given above, the committee considered more than just the design of information and communication systems, a critically important topic in itself. Since the point of network-centric operations is to empower the entire naval force to maximize the effectiveness of its operations, this examination of network-centric operations has been extended to include the entire naval force system encompassed by the committee's

definition of network-centric operations, and network-centric operations are treated in terms of mission accomplishment by that system.

When the committee examined the naval forces' mission spectrum from this point of view, it realized that the force capability has not developed rapidly enough in all mission areas since the end of the Cold War to keep up with the ensuing profound change of emphasis in overall mission orientation (see discussion in Box 1.2). As a consequence, attention is devoted in several parts of this report to the power projection mission, and network-centric operations are discussed in terms of the subsystems and components that will enable the naval force network to succeed in that mission.

Finally, as requested in the terms of reference, attention is also given to the demands that the move to network-centric operations will make on the business practices and organization of the Department of the Navy, including the problems associated with the training, retention, and promotion of naval personnel in the developing network-centric operations environment, as well as the unprecedented opportunities offered by the new information and networking technologies.

In the following overview of study results, the recommendations associated with each major topic are presented following the discussion of that topic. Additional recommendations are offered in Chapters 2 through 7.

1.2 LEADING THE TRANSFORMATION TO NETWORK-CENTRIC OPERATIONS

1.2.1 Integrated Systems for Operations

Network-centric operations represent a new approach to warfighting. When that approach and its elements are discussed, familiar terms come to be used in new ways to deal with new concepts.

In network-centric operations, a set of assets, balanced in their design and acquisition so as to be integrated with one another, must operate together effectively as one complete system to accomplish a mission. The assets assembled in such a *network-centric operations (NCO) system* encompass naval force combat, support, and command, control, communication, computing, intelligence, surveillance, and reconnaissance (C4ISR) elements and subsystems, integrated into an *operational and combat network*. Such subsystems will be designed and acquired to meet specific requirements of their tasks in the overall mission. For example, a fleet and amphibious force assembled for an expeditionary operation along the littoral will comprise subsystems designed for power projection but will also include antiair, antimissile, and antisubmarine subsystems to protect the naval force while it is projecting power ashore, as well as logistics subsystems to support the forces at sea and ashore.

The subsystems' *components* will be ships, aircraft, missiles, communications, and other parts of the C4ISR network. These components will continue to

Box 1.2 Network-Centric Operations for Power Projection

The naval forces have always had the missions of deterrence, forward presence, sea and air control, and power projection. During the Cold War the emphasis was on strategic deterrence, protection of the sea transit of reinforcements to the European theater, and the ability, under the maritime strategy of the 1980s, to bring naval aviation within striking distance of the Soviet Union. Because the Soviet threats to the fleet were severe enough to keep it from carrying out those missions, defensive operations were of critical importance and led to networked operations in antisubmarine warfare (ASW) and Fleet Air Defense. The ASW network included fixed arrays such as the Sonar Ocean Surveillance Underwater System, as well as sensor and attack capabilities by maritime patrol aircraft, carrier-based aircraft, and ship- and submarine-based ASW systems, all operated in a cooperative manner to find and neutralize Soviet submarines. The Fleet Air Defense system included the Outer Air Battle systems, Aegis, and ultimately the cooperative engagement capability to counter low, stealthy, or supersonic antiship cruise missiles.

Since the end of the Cold War the naval forces have turned their attention to expeditionary warfare and military operations other than war in the world's littoral zones, especially those of the Eurasian and African land masses. As threats against the fleet and movement over the seas have diminished, emphasis has shifted to the forward presence and power projection missions. In the words of the Chief of Naval Operations, Admiral Jay Johnson, USN, "The purpose of Naval Forces is to influence directly and decisively, events ashore from the sea—anytime, anywhere."[1] Although much work remains to be done in the other mission areas, it became apparent to the committee during its study that elements of the power projection mission have lagged significantly and now require renewed emphasis. These mission elements may be grouped according to the following phases of a campaign:

- Preparing the battlespace: This involves integrated battlespace sensing and sea- and air-launched strikes against inland targets using fleet firepower and information warfare;
- Landing the force: This includes countermine warfare, landing the Marines ashore in their developing Operational Maneuver From the Sea mode of operation, and providing them with close air support during the landing;
- Engaging the enemy; and
- Supporting the force ashore: This entails supplying fire support and logistic support from the sea.

[1]Sestak, RADM Joseph A., Jr., USN, Director of Strategy and Policy Division. 1999. "A Maritime Concept for the Information Age," brief presented to the Naval Studies Board on November 18, Office of the Chief of Naval Operations (N51), Washington, D.C.

involve research, development, and acquisition efforts involving extensive resources.

Although this characterization of the NCO system might imply a classical system-subsystem-component hierarchy, it must be recognized that NCO systems may differ in composition, but not in concept, depending on the mission or the circumstances. Thus there can be different NCO systems for various purposes—e.g., for forward presence and deterrence, or for fighting a major theater war—sometimes operating simultaneously within a global network.

To support such adaptations of the overall system concept, different stages of system design and acquisition will require different types of system-oriented analyses. Development and experimentation in the field to perfect various NCO concepts require *operational analyses*. System planning, programming, and budgeting, as well as making trade-offs among mission-oriented subsystems of what will become NCO systems, require *systems analyses*. Building the components and subsystems to work together satisfactorily requires *system engineering*.

Network-centric operations represent a new paradigm for the naval forces, which no longer will be considered in terms of assemblages of ships, aircraft, Marine units, and weapons drawn together to fight battles. Rather, the platforms, Marine units, and weapons will be part of a network integrated into a system to carry out a mission, supported by a common command and information infrastructure. All the naval forces, at all command levels, will be involved in and affected by this change.

Network-centric operations are characterized by the rapid and effective acquisition, processing, and exchange of mission-essential information among decision makers at all command levels, enabling them to operate from the same verified knowledge base, kept current according to the temporal needs of the commanders at the different levels. This approach will enable the naval forces to perform collaborative planning and to achieve rapid, decentralized execution of joint actions, based on the most accurate and timely situational and targeting knowledge available. It will enable them to focus the maneuvers and fire of widely dispersed forces to carry out assigned missions rapidly and with great economy of force.

Network-centric operations systems include, in addition to the people who use the information in the network to direct operations, the naval forces' platforms, weapons, Marine units, and all the parts of the command and information structure within which they fit and that binds them together and guides their operations. Joint Service elements or forces and coalition forces operating with the naval forces must also be included. In any mission assignment, from peacetime engagement to combat in a major theater war, NCO systems encompass, as appropriate, all operations from a single weapon engaging a single target to a regional force including one or more fleets and Marine expeditionary forces that might be operating anywhere in the world.

The command and information parts of NCO systems include all the sensors

and their platforms, from shore-based installations through ships, manned and unmanned aircraft, and spacecraft; processing and display subsystems; communication links; common supporting software; the standards, rules, and procedures that lend structure to the network and enable seamless, integrated functioning of all its parts; and the people at all levels, in joint and combined forces, who use the information in carrying out their tasks and missions and who maintain and operate the system's infrastructure. The Naval Command and Information Infrastructure (NCII), meshed with and functioning as part of a joint and national infrastructure, must provide a functional framework for establishing and maintaining the relationships and for transferring information among all the system parts, and for coordinating functions across all the platforms and force units in the joint and combined environment.

Figure 1.1 summarizes the comprehensive nature of network-centric operations systems; that view guided the committee's deliberations.

1.2.2 Creating Network-Centric Operations Systems

Transforming the naval forces from platform-centric to network-centric design and operations will require a disciplined approach to developing very-large-scale integrated systems. New concepts of operation embodying new technical capabilities will have to be developed and then tested in the field, with the test results used to refine the concepts continually and adapt them to changing conditions of threat, environment, and technological advance. This means using up-front, empirically founded operational and system analyses to set system performance, cost, and schedule requirements based on emerging concepts of opera-

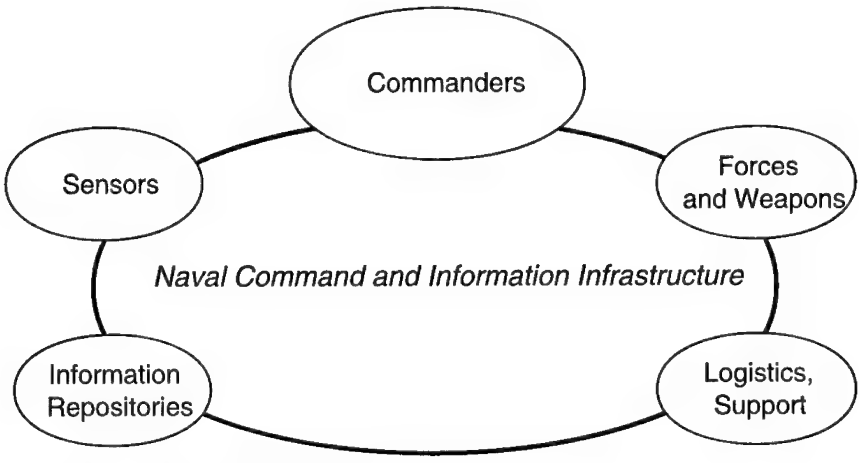

FIGURE 1.1 An NCO system structure.

tion; performing studies of the trade-offs in alternative approaches to system design; selecting and documenting a baseline approach; managing the design and implementation of the system according to the planned schedule and cost targets, while being adaptable to unforeseen contingencies; verifying that the design meets requirements; and maintaining meticulous documentation of the entire process.

To implement the system, responsible organizations must first devise joint concepts of how network-centric operations would work. These concepts will form the starting point for the spiral development process described below. Within the naval forces, the Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) have assigned such development responsibility to the Navy Warfare Development Command (NWDC) and the Marine Corps Combat Development Command (MCCDC), respectively. To date, these organizations have been functioning more or less independently, each devising concepts for its parent Service. However, since network-centric operations will be joint and will most likely involve coalition partners, the NWDC and MCCDC must work together and must incorporate the inputs from other Services and agencies, as well as from potential coalition partners, into their work.

The implementation of network-centric operations does not start from a zero base. The naval forces are faced with transforming today's systems—including "legacy" subsystems, new ones entering service or under development for future service, and also elements of subsystems of other Services, National agencies, and possibly coalition partners—into new, all-inclusive systems. All of these subsystems and their components must be able to operate together, even if they were not originally designed to do so. All must be accounted for in devising network-centric concepts of operation and in designing the systems that will support them.

One of the greatest problems in shifting from today's platform-centric operational concepts to tomorrow's network-centric operational concepts is to ensure interoperability among the subsystems and components of the fleet and the Marine forces as well as of joint and coalition forces. The forces can operate to their full potential only if all subsystems and information network components can operate smoothly and seamlessly together. In the current context "interoperability" does not necessarily mean that the characteristics of all subsystems and components must match at the level of waveforms and data formats. Interoperability means that the subsystems must be able to transfer raw or processed data among themselves by any means that can be made available, from actually having the common waveforms and data formats to using standard interfaces or intermediate black boxes enabling translation from one to another.

Ensuring interoperability will be a very complex, technically intensive task involving network protocols, data standards, consistency algorithms, and many other aspects of network design, as well as numerous procedural matters. The subsystem mix will evolve and will be different from the one that exists today.

Eventually, today's legacy subsystems, most of which were not designed for interoperability, will give way to subsystems that are so designed, but only if the networks are configured appropriately now. Even so, different subsystem and component upgrades or replacements will have different time frames for development and installation, so that interface standards will have to ensure their proper meshing into overall systems as they are created. As network-centric operations systems are constituted, all will have to be based on the same command and information framework (the NCII) and all will have to be interoperable.

Network-centric operations must be based on the transformation of both raw and processed data into "knowledge." That is, the masses of information from often dispersed sources must be integrated, interpreted, and presented to combat leaders in a common operational picture that will enable them to discern meaningful patterns of enemy activity in conditions that are disordered and confused, and to act effectively on that information. This knowledge, coupled with their own experience, judgment, and intuition, will allow well-trained leaders to adapt to the situation at hand, identifying and exploiting enemy vulnerabilities while guarding against exploitation of their own. All the design concepts, equipment, and supporting elements of NCO systems must support this capability.

Essential as they are, analytical methods alone are insufficient for the design of systems of this complexity. Actual experimentation by the fleet and Marine force elements is required, to learn how legacy subsystems and their components will operate together with existing or testbed versions of new subsystems and components and to devise concepts of operation using the new and the legacy subsystems and components in the actual operational environment. When such a development process, part of what has been called spiral development, is used, new equipment and concepts can be incorporated into the fleet and the Marine forces based on validated concepts of operation.

In spiral development, equipment and operational concepts are designed, tested, and then refined or redesigned based on the results of real-world experiments. Concepts and components whose effectiveness is demonstrated in the experiments are incorporated into the operational forces, while those requiring improvement enter the next phase of the development spiral. This process will ensure that NCO systems remain vital and current, evolving continuously to incorporate new technology in a constantly changing environment. The process of spiral development can be expected to converge on successive versions of NCO systems that incorporate major force elements far more rapidly than do traditional processes that call for the full development of subsystems and components before outfitting the forces. Also, it will help to identify and resolve interoperability problems in time to avoid large and expensive retrofit programs.

The shift from platform-centric to network-centric thinking and operation of naval forces will require a shift in the mind-sets, culture, and ways of doing business of all the naval forces (and, indeed, in their connections to other Services and National agencies). To shorten the interval between learning about situations

and opposition activity from a variety of information sources both within and outside the naval forces, and taking necessary action, command relationships will have to adapt to the exigencies of operations. Achieving the required speed of action will require flattening of the command hierarchy at certain times and preserving the familiar hierarchy at others. Such profound transformation can only be effected through continuous commitment, attention, and guidance from the top levels of naval force leadership.

1.2.3 Recommendations Regarding the Transformation to Network-Centric Operations

1. Network-centric operations planning, design, and management should emphasize mission success in the network-centric operations mode, not the physical aspects of the C4ISR network per se.

2. The Department of the Navy and its component Services should take a mission-driven, integrated approach with a total-system view to achieve success in transforming the naval forces from platform-centric to network-centric operations. Specific steps to achieve this are included in Section 1.5.

3. The CNO and the CMC should give the Navy Warfare Development Command and the Marine Corps Combat Development Command the responsibility of working together to devise joint concepts and doctrine for network-centric operations for the naval forces as a whole, and to incorporate joint and coalition aspects of such operations in their concepts.

4. The spiral development approach involving the design-test-design of new software and equipment and model-test-model to devise new joint concepts and their testing in fleet and Marine units should be adopted as a standard mechanism for achieving network-centric operations systems.

1.3 INTEGRATING FORCE ELEMENTS: A MISSION-SPECIFIC STUDY OF POWER PROJECTION

1.3.1 Mission Orientation

Network-centric operations systems comprise a number of subsystems, each designed and engineered to accomplish a military purpose. These subsystems are networks of components such as sensors, weapons, command elements, and mission-specific communications, tied together by the NCII. First it is necessary to understand the characteristics of the components and the interdependencies of component performance and subsystem performance.

The four missions of the U.S. Navy are illustrated in Figure 1.2, which summarizes the major components in the Navy's integrated warfare architecture (IWAR) process. The subsystems for strike and fire support missions against land targets are used here as example subsystems to accord with the selected

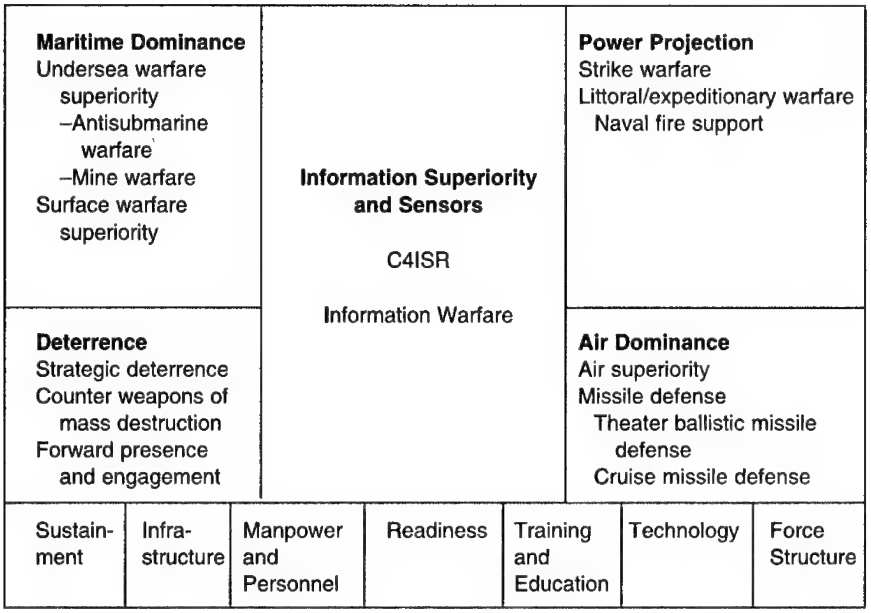

FIGURE 1.2 Naval forces integrated warfare architecture (IWAR) structure. The four fundamental naval force missions are listed in the side columns; all the remainder are essential for carrying them out. (Information superiority and sensors are enablers of all four missions.)

emphasis on the power projection mission described in the introduction to this overview and integrated into the detailed discussion in Chapter 3.

1.3.2 Critical System Needs

Developing the capability for effective power projection by the Navy and Marine Corps requires that the mission-specific networked operations that have already been developed must be integrated into a comprehensive NCO system structure (see Figure 1.1). Under OMFTS, landing (and supporting) forces expands the battlespace deeper into opposition territory and more widely along the littoral. Elements of the total force may be widely dispersed, requiring that they be firmly and effectively linked through the command and information infrastructure. Barriers to landing, such as minefields and proliferated shoulder-fired surface-to-air missiles, must be overcome rapidly. Greater involvement with civilian populations and the need for rapid closure and success and for minimization of U.S. and collateral casualties increase the criticality of accurate, timely fire support from the sea.

Such performance cannot be achieved unless intelligence, targeting, launch platforms, weapons, and postattack assessment are integrated into a fully connected, robust operational and combat network covering every phase of an expeditionary campaign: preparing the battlespace (strike warfare); landing the force (mine clearing, suppression of enemy air defenses (SEAD), amphibious and air-landed operations); engaging the enemy (fire support to forces on the ground); supporting the force ashore (logistics from sea and land); consolidating the position (civic and psychological operations, defending against counterattack); and handing off to follow-on forces and debarking the Marines who were the landing force. Moreover, since naval force operations involve the simultaneous execution of many activities in many mission areas, networked capabilities in other areas, such as ASW and CEC, must be integrated with those for power projection to achieve network-centric operations for an entire force in a total operational context. Creation of such a force-wide NCO capability requires multiple lines of research and development (R&D), procurement, and organizational effort, including the spiral development process described above.

A critical aspect of power projection is the delivery of accurate and timely firepower from the sea on targets ashore, either for strike or for fire support of Marines (and other forces) there. In the past, weapons were typically developed largely independently of the targeting means and of the means for penetrating defenses to deliver the weapons or to assess their effects once delivered. Network-centric operations will require effective integration of sensors and target acquisition, navigation, and weapons to account for all the factors shown in Figure 1.3 and for multiple feedback loops (which have been eliminated from the diagram for simplicity of illustration).

Some specific component needs are discussed below.

1.3.2.1 Sensors and Target Acquisition

To provide all the information needed for force movement and weapon delivery, sensors will have to be linked, as, for example, distributed radars are used in CEC, electronic intelligence sensors are used to guide SEAD attacks, and the Joint Surveillance and Target Attack Radar System (JSTARS) is used to cue specific weapon-targeting sensors against ground forces. Figure 1.4 illustrates how triangulation can reduce target location uncertainty, provided that the sensor positions are precisely known and the observations are synchronized. Coherent processing of detailed sensor observations can produce identified tracks in situations where no single sensor could perform an unambiguous detection, identification, or track. (Although two radar sensors are shown in Figure 1.4, sensors in different frequency domains that meet the above conditions can yield similar results, or better if they contribute to more positive target identification.)

The importance of real-time fusing of multiple sensor outputs as a driver for the target engagement architecture cannot be overemphasized; it is fundamental

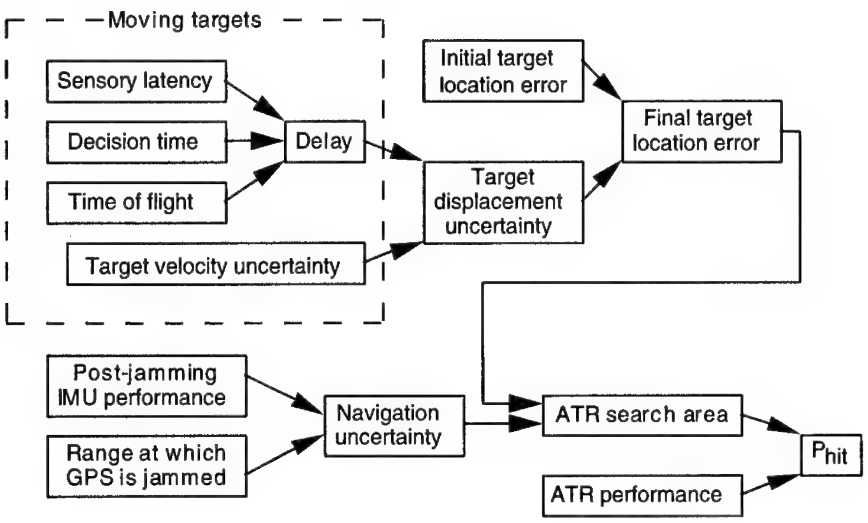

FIGURE 1.3 System factors in delivering firepower ashore without in-flight links to targeting sensors. ATR, automatic target recognition; IMU, inertial measurement unit; GPS, Global Positioning System; P_{hit}, probability of hit.

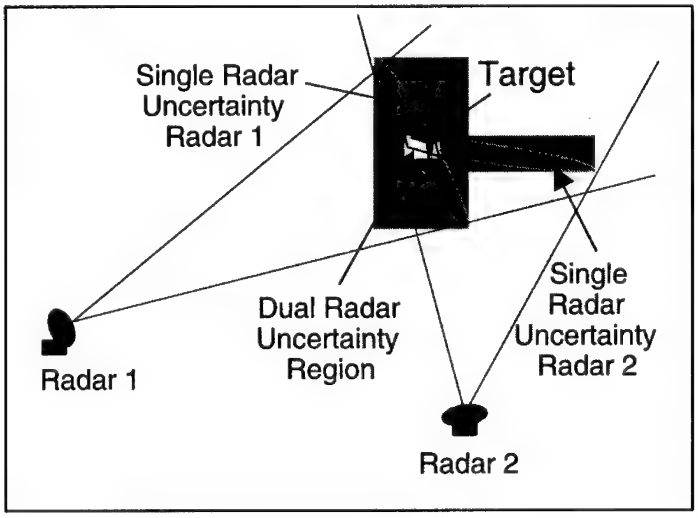

FIGURE 1.4 Reducing target location error with linked cooperating sensors in common coordinates.

to bringing network-centric operations to the point where U.S. forces meet the enemy. The change in architecture brought about by linked sensors is illustrated schematically in Figure 1.5.

The implications for change in the nature of combat engagement as illustrated in Figure 1.5 are profound. On a single platform it is relatively easy to close the observe, orient, decide, and act (OODA) loop. The challenge in network-centric operations is to enable OODA loops that span space and time as effectively and as rapidly for dispersed force elements as for a single platform, particularly when some sensors may be involved in multiple loops. Any sensor and processor with useful data or information will provide it for anyone who can use it, and the provider may not know who the user is nor the user who the provider is. In the large, however, the operation of the network will remain a closed loop in that information will lead to action, and the mission decision maker—the one who decides what the target is—will have to know that the target was engaged and the outcome of the engagement, as a condition for deciding on further action.

In addition to having to be linked, sensors require continual improvement. Phenomenology in all spectral domains must be explored to exploit multiple sensing paths to the greatest extent possible, both physically and economically, and the quest must continue for automatic recognition of targets that are detected. Automatic target recognition (ATR) will, when it is achieved, aid not only in finding targets in noisy backgrounds but also in defeating the effects of countermeasures to accurate navigation and guidance of weapons. It will also reduce the number of personnel needed for the information-processing parts of the NCII and other information operations.

The use of unmanned aerial vehicles (UAVs) for surveillance; target detection, recognition, and location; and postattack reconnaissance for effectiveness

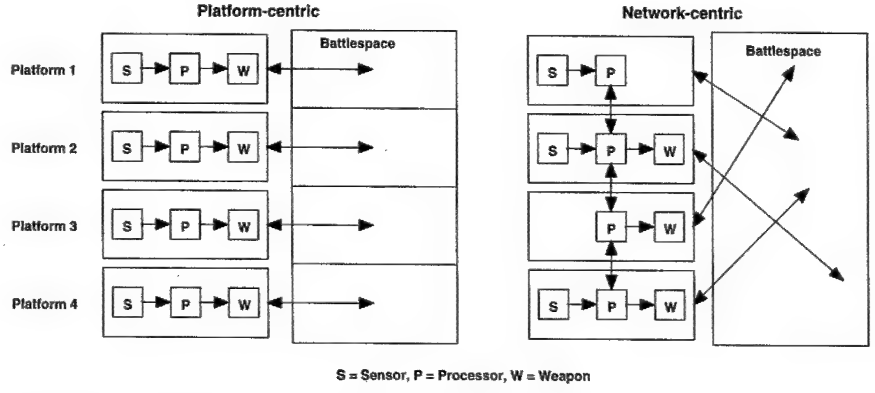

FIGURE 1.5 Platform-centric versus network-centric architecture.

assessment has been accelerated during military operations in the former Yugoslavia, where UAVs were effectively utilized as joint and coalition-based assets. In addition, the Marines will have a continuing need for short-range, organic UAVs for close-in targeting and to elevate communications relays.

1.3.2.2 Navigation

The problem of Global Positioning System (GPS) jamming will become more acute as weapon ranges and times of flight increase and will have to be overcome. No single technique will make GPS-aided weapon guidance invulnerable to GPS jamming. Practical solutions are likely to involve a combination of cheaper, precise inertial measurement units (IMUs), better target acquisition (including ATR), improved satellite signals and receiver signal processing, directive arrays of antenna elements, and the correlation of multiple signals and sources. Shorter times of flight, achieved by increasing weapon speed, together with improved, low-cost IMUs, can reduce reliance on GPS in the endgame against targets whose locations have been determined a priori. For moving targets being attacked by weapons without update links, time of flight and ATR go hand in hand; shorter delays make the ATR task easier. However, update links to enable the "forward pass" mode, in which weapons are given continually updated target location information after they are launched, are preferred for attacking moving targets, and when such links (and the sensors behind them) are available, ATR becomes much less important. Also, targeting and weapon delivery must be locked in the same reference grid to minimize the error due to target location inaccuracies.

1.3.2.3 Weapons

Naval force weapons are being made more accurate to reduce the need to reattack targets and to reduce collateral damage. The combination of greater accuracy and improved warhead lethality will allow lighter warheads, thereby increasing the range of weapon delivery systems. Weapons will need shorter times of flight to engage fleeting, moving, or highly threatening targets, despite the longer standoff needed to enhance the safety of launching platforms. This will be achievable by launching from advanced aircraft, often at supersonic speed, and by rocket propulsion of air- and sea-launched weapons. For the most effective results in some parts of the strike and fire support missions (e.g., attacks against concentrated targets embedded in population centers or very close to U.S. ground forces), accuracy at the target will have to be improved from the currently specified 13-meter circular error of probability (CEP) to 1 or 2 meters, including target location error. Additionally, the much greater use of precision weaponry will require that, notwithstanding all the weapon improvements called for, weapon costs be reduced significantly to achieve sustainability in a campaign.

In considering the design conditions for an overall subsystem, the performance goals for the components of the subsystem must be traded off against one another on the basis of mission performance. For example, GPS jam resistance can be traded off against ATR performance, guidance accuracy can be traded off against warhead radius of lethality, sensor latency can be traded off against weapon time of flight, and the reduced sensor latency afforded by data links to weapons in flight can be traded off against target location and guidance accuracy.

Network-centric operations require an intimate connection among all the sensing, processing, navigational, and weapon components of the NCO power projection system. Thus, all must conform to the compatibility and interface standards of the NCII. Currently there is no mechanism to coordinate the development of Navy and Marine Corps doctrine and apparatus for joint littoral operations or to coordinate such functions as tracking and network control.

Success in the power projection mission will require that all the areas touched on above and elaborated in Chapter 3, and many of the related areas discussed there, be supported with resources and worked on simultaneously in a fully integrated fashion.

The fielding of improved subsystems will have to be integrated in any NCO system by continually improving subsystems to support the force. Also, the United States may have more than one NCO system or force operating simultaneously in different parts of the world, or even in the same theater of operations. There must be an overall infrastructure—the NCII—with joint and coalition connections, to ensure consistency and interoperability among such far-flung assets, from local tactical networks to major commands, in a global naval force network.

1.3.3 Recommendations Regarding the Integration of Force Elements for the Power Projection Mission

1. In all Department of the Navy planning and acquisition activities, the integration of components for the power projection mission, as well as the integration of the power projection subsystems with the subsystems for other naval force missions such as air and maritime dominance, should be considered as the combination of related parts of a total NCO system, including all the component functions and equipment described above. This includes the naval forces' continuing efforts in the areas of countermine and amphibious warfare, and other efforts.

2. The Department of the Navy should engineer the strike and naval fire support subsystems of NCO systems in an end-to-end fashion. This includes the capability to sense, track, and hit high-priority relocatable or mobile targets with ad hoc or on-call fire and then to assess the results of strike and naval fire support operations in near-real time. Engineering studies and tests should be conducted to define effective, affordable, and balanced major subsystems in all mission areas.

3. System engineering should be performed to determine what combinations of improvements would be required to overcome the effects of foreseeable GPS jamming. Technology base funding and demonstration funding should be made available to determine whether these improvements are attainable.

4. A number of technology directions should be pursued in furtherance of the power projection mission:

a. Diversity of sensor phenomenology and locations should be sought; new sensors should provide for cooperative behavior and participation in ad hoc networks;

b. Organic airborne moving target indicator (MTI) sensors should be considered for guiding precision weapons fired from over the horizon toward moving targets in the forward-pass mode; it should be ensured that closed-loop control in the forward-pass mode is not foreclosed in the design of sensors and weapons or by the concepts for their targeting;

c. Technology for better long-range identification of targets (including ATR) should be sought; in this regard, the Department of the Navy should interact more strongly with Defense Advanced Research Projects Agency (DARPA) programs; and

d. Technology to achieve affordable antennas with adequate gain, bandwidth, and flexibility, and that maintain low observability of the platform, should be sought. A particular challenge is to provide multiple-beam, directional, shared large-aperture antennas on major Navy platforms to serve the needs of the NCII as well as weapon systems.

5. The Department of the Navy should move more urgently toward providing the naval forces the capability to acquire data from theater and National sensors.

6. As part of the assignment to NWDC and MCCDC to jointly devise NCO concepts for the naval forces as a whole, the relationship between the two organizations should be formalized and institutionalized to encompass NCO innovation; tactics, techniques, and procedures; and doctrine for operations in the littorals. In particular, they should reach agreement on the need for a family of short-time-of-flight, over-the-horizon weapons and concepts for their targeting.

Many additional recommendations are included in the main body of this report, at a more detailed level than is appropriate for this overview. Those recommendations aim at improving specific sensor and weapon technologies, thereby greatly enhancing the naval forces' ability to carry out effective sea-launched strike missions and to provide highly responsive, long-range, affordable, sustainable, accurate, high-volume ship- and aircraft-launched supporting fire. These detailed recommendations are as essential to successful achievement of the aims of NCO systems as are the higher-level recommendations included in this overview.

1.4 DESIGNING A COMMON COMMAND AND INFORMATION INFRASTRUCTURE

1.4.1 The Naval Command and Information Infrastructure Concept

The Naval Command and Information Infrastructure will become the enabling framework for network-centric operations. The NCII includes the communications trunk lines, terminals, tactical networks, central processing facilities, common support applications, and Department of Defense (DOD)-wide and commercial standards, rules, and procedures that will enable the flow of raw and processed information and commands among units at all levels of command. Its attributes are listed in Figure 1.6, an expansion of Figure 1.1.

All the Services are striving to achieve the capability to share information, based in large measure on the Internet paradigm. The Internet's robust, networked communications base enables rapid, ready, and flexible access to information and supports the applications that provide information and services to a widely dispersed user population. Some top-down principles and standards are necessary for the communications base so that the applications can easily use it and so that users can interoperate with applications. In the Internet applications are developed from the bottom up by a diverse developer population. Thus there is a broad base for innovation, an important factor contributing to the utility of the Internet. The point for the NCII is that it should use standards that will permit its applications to come from diverse sources to serve a diverse set of users. In this respect, the Internet is the best model available to describe the design approach for the NCII.

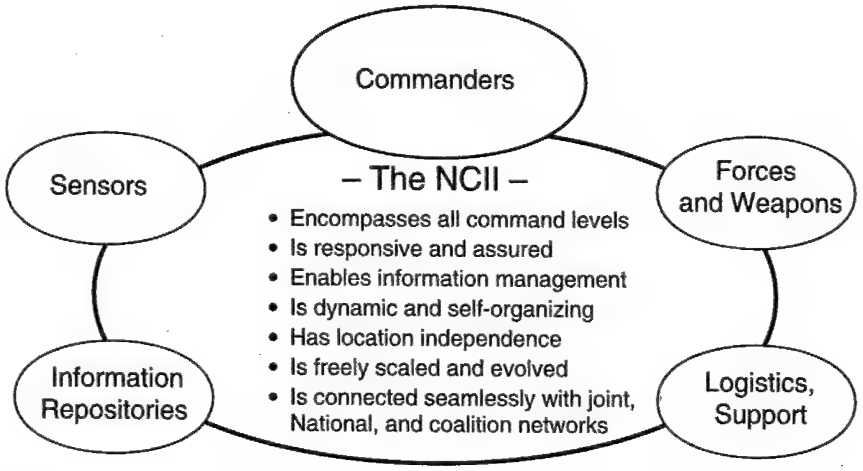

FIGURE 1.6 Attributes of the Naval Command and Information Infrastructure.

As with the Internet, users of the NCII will not be satisfied with, nor will their needs be met by, some fixed, predefined set of information. The uncertainty as to the type and location of future military operations ensures that. Relatedly, different operators may vary in their approach to a situation, and hence in their information needs. Furthermore, the manner in which information is used in the NCII will change continually as operational concepts are refined and new technologies introduced. For all these reasons, a central notion of the NCII is that it be flexible, adaptable, and evolvable in meeting the needs of its users.

While the NCII includes tactical networks and allows for widespread dissemination of information, it must also accommodate the need of commanders for some degree of control over such dissemination, for, among other things, security purposes and bandwidth management. This management of information dissemination facilitates and allows for decentralization of command, but at the same time it allows for the centralized collection of information and hence for greater centralization of authority. There is no one generally appropriate point to aim for on this centralization-decentralization spectrum; it will depend on the nature of the military operation. The NCII must be able to support varying modes of command.

The NCII is conceived not only as carrying long-haul traffic but also as enabling short-haul and tactical information acquisition, processing, and transfer. The acquisition of raw information and its processing into an accurate understanding of the current details of environments, forces, targets, and maneuvers must be treated separately from the transport (communication) of the information and the commands based on it. The NCII provides for the integration of the acquisition and processing mechanisms and provides the transport for information and command at all levels, from major force operations to single target-shooter engagements.

The mechanisms for transporting information for many services and functions will rely heavily on civilian, commercial systems. Purely military functions will appear more in the information processing and command parts of the NCII, where security and the special characteristics of military operations are driving factors, although purely military functional capabilities will be built in good measure from commercial sources and technology.

The NCII should be recognized as the naval force portion of an information infrastructure that is interwoven with, shares common components with, and adheres to the same set of standards as other Service, National, and, when appropriate coalition networks, such that all function as a global whole. Thus, the NCII will have to be built to standards established by others, although the Department of the Navy should play a part in developing some of the standards. Since the network will have commercial components, the standards will also have to be compatible with and often the same as commercial standards. These standards, and the rules and coordinated operational procedures that go with them, will be the only means by which full interoperability can be achieved. Full inter-

operability will be essential to bring all the benefits and advantages of network-centric operations to fruition.

Tactical networks are of special concern since they pose the greatest challenge to the goal of using standard, Internet-based networking technology throughout the naval infrastructure. The Navy and the Assistant Secretary of Defense for C3I (ASD (C3I)) have argued that this class of radio networks must necessarily be based on nonstandard, military-developed technology to meet the tight time constraints and extreme reliability that tactical communications require. Accordingly, the current Navy networking architecture defines two special-purpose tactical radio networks in addition to the standards-based Joint Planning Network: the Joint Data Network (actually, the Joint Tactical Information Distribution System (JTIDS)) and the Joint Composite Tracking Network (actually, CEC).[7] Although the Navy and ASD (C3I) argument has merit, the committee concluded that there are greater advantages in extending a uniform, open, standards-based network architecture across the entire naval infrastructure, including the tactical networks. The committee envisions a network in which tactical data communications are provided via the NCII standards, including a standardized naming and addressing scheme and data transport using the Internet Protocol (IP). The committee believes that advancing commercial technology will make it possible to remove technical impediments to allowing any type of data to be conveyed across any type of radio link.[8] If an Internet-based architecture is adopted, new types of tactical services can be rapidly deployed across in-place radios.

It is important to note that the committee does not believe that all types of traffic should be allowed to cross any tactical radio network freely. Quite the contrary: Strict controls will be necessary at the connection points between the tactical and nontactical portions of the NCII. These controls will ensure that only authorized types of traffic are allowed onto the tactical networks, and hence they will provide continued guarantees that the tactical networks can provide highly reliable, low-latency data services. These controls will also aid in providing security boundaries (i.e., firewalls) within the NCII as part of the network defense in depth discussed in Section 1.4.2.

In the end, it is likely that a few tactical networks will remain outside the NCII for some combination of technical and economic reasons. Such outlying tactical networks can be connected into the Internet-based NCII via IP-capable

[7]Furthermore, as far as the committee can tell, this focus on the Joint Data and Joint Composite Tracking Networks omits consideration of all other tactical communications networks currently employed by the Navy that are part of the overall information transfer capability. These include various sensor links—e.g., for MTI and synthetic aperture radar data—and links to weapons control systems—e.g., ultrahigh frequency satellite communications target location updates for Tomahawk.

[8]Approaches to this are described in some detail in Appendix E.

gateways so that they can still enjoy the advantages of being part of the overall, seamless naval network infrastructure.

It is important to understand that the NCII itself does not represent a major new investment. Rather, it requires an investment of resources sufficient to integrate the many subsystems and components, some of which exist, some of which are being developed, and some of which are or may be planned, in a way that provides guidance and structure for an overarching concept for information support to network-centric operations.

The general composition of the NCII is illustrated by its functional architecture, shown in Figure 1.7 and discussed in detail in Chapter 4. The starting premise of this functional architecture is the need to support the warfighting decision process extending across all levels of command, to include those engaged in actual weapons delivery. Shown in the top half of the figure are the functional capabilities (collection management, etc.) that gather and generate information to support the decision process, and then see that the decisions are conveyed to their appropriate recipients. Across the bottom of the figure are the supporting resources (communications, etc.) used by the "upper level" functional capabilities.

Collection management determines the tasking of sensors to collect data. The information exploitation and integration function takes the initial data and refines the information by correlating, fusing, and aggregating it. Information request and dissemination management provides information based on user-specified requests for a given type of information. Its operation is transparent in that users do not have to know the details of where the information is located. This function will also provide information to users based on the directions of any other authorized party. Information presentation and decision support includes the graphical means for displaying information to users and the set of automated

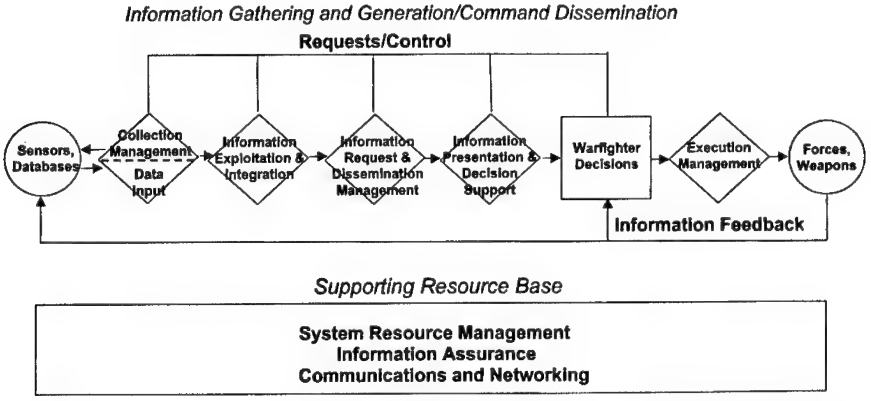

FIGURE 1.7 Functional architecture of the Naval Command and Information Infrastructure.

tools that allows users to manipulate information for the purposes of making a decision. Execution management supports delivery of decisions to the intended recipients and allows for dynamic adaptation of those decisions in the light of rapidly changing events. The other functions illustrated in Figure 1.7 are self-evident.

1.4.2 Information Assurance Within the NCII

"Information assurance" is the term used in this report to describe how threats to and vulnerabilities of the NCII must be addressed to ensure the integrity of information and the timeliness and continuity of its flow for network-centric operations as a whole.

The NCII, like all information networks in the modern age, must routinely exhibit high reliability and must include safeguards against system failures due to overload, loss of critical nodes as a result of enemy action, and other operational factors. It will also face many threats to the quantity, quality, integrity, and continuous flow of the information it manages and provides, and it will have many vulnerabilities. Both the threats and the vulnerabilities are too numerous to elucidate in this summary discussion. They are noted briefly here and are described in detail, along with potential defenses and countermeasures, in Chapter 5.

Critical vulnerabilities for tactical networks are spoofing, jamming and other interruptions, interception, and ground terminal capture. Important sources of weakness in the NCII transport elements will derive from the use of commercial subsystems and from the outsourcing of important elements of the transport operations, and also from the need to connect with and share information with coalition partners. The key strength of the NCII in allowing the connection of disparate networks and functions is also, however, a source of risk. Among these connections is that linking the fleets' operational networks, in which a degree of secrecy and control can be maintained, with the naval force business networks that are essential for the logistic support of the fleet and that must be open to both the naval forces at sea and their shoreside commercial connections. A critical vulnerability in the nontransport part of the NCII derives from the threat posed by the potential malicious insider, who could, working alone or with outside adversaries, cause serious disruption to network-centric operations.

NCII information assurance must be achieved throughout the information infrastructure, including wireless links. In the design of the NCII, all components must be treated as vulnerable, and security vulnerabilities must be anticipated in any system component and even in any given protection mechanism. Overall, to meet the threats and mitigate the vulnerabilities, a defense in depth is required. It consists of three elements: prevention; detection of attack, assessment of the damage, and remedying of the effects of the attack; and robustness in its ability to tolerate penetrations.

Today, because of technology shortfalls at each level of the defense-in-depth strategy, it is not possible to completely implement such a strategy. However, in some cases steps that do not depend on technological remedies can be effective. For example, in a crisis certain functions may be considered so critical that any risk to their timely and correct functioning is intolerable. In such cases, the decision may be to not connect, and to use an air-gap defense (which inserts a deliberate break, to be connected by manual action, in a link of the network). Reducing the risk of damage by a malicious insider might be accomplished by reducing the scope of access and control available to any single individual, and by requiring two- (or more) person control of key functions. Monitoring user activities, coupled with exploring observed anomalies, is another risk-reduction technique.

Red teaming is often prescribed for exposing a system's vulnerabilities and weaknesses so that they can be remedied. However, it is important to understand and capitalize on red teaming's strengths while understanding the limitations of its use. Red teaming proves not to be a preferred way of discovering system vulnerabilities or learning how to mitigate threats, because the red teams come from the same culture that created the system. Red teaming's primary benefits are that it is the best tool for raising the level of security awareness within an organization and that it is useful as a method for ensuring that correct security configurations are maintained for the system. Red teaming for these purposes can be carried out by a system's security staff on a periodic basis.

In its review, the committee found that information assurance for the NCII is not receiving appropriate attention at high enough levels within the Department of the Navy to ensure that this critical problem area is managed in a manner consistent with its importance to successful network-centric operations. There is no single individual in the Department of the Navy charged with the responsibility for information assurance. Further, the Navy Department has no overall plan for information network security in its tactical networks. Mitigation of vulnerabilities will come from many measures in the defense in depth, with support from continual red teaming, but the organizational problems will have to be remedied as well.

In addition, because of the likelihood of attack on the NCII or its operational degradation, it is imperative that naval forces train for situations with impaired NCII function. Not only must the NCII system staff learn to quickly restore service, but the operational forces must also learn to deal with system failures. Beyond that, in recognition of the vulnerabilities the forces should be shaped such that they can fall back to operational modes that are at least as good as those that preceded network-centric operations. For example, the naval forces have a tradition of developing operational workarounds for loss or degradation of radio frequency communications in tactical operations. The same should be done for the NCII so that naval forces will be prepared to deal with these likely situations in practice.

In the spiral development process, especially in the experiments and proof-of-concept exercises that will attend the development of concepts of operation, the opportunity will exist to probe for the most logical vulnerabilities (e.g., jamming of tactical networks) and to design appropriate redundancies and fallback modes of operation.

Is it worth accepting all the vulnerabilities and the attending risks, as well as the cost and operational penalties of anticipating and remedying them? This is a question that cannot currently be quantified. However, in all recent military endeavors, including the Gulf War and operations in the Balkans, and in endeavors throughout the national and even the global economy, the gains are seen as being so great that the risks are accepted even while mitigation attempts are undertaken and their costs incurred. The trends in technology, force size and utilization, and U.S. global responsibilities are such that network-centric operations offer the only means of achieving the necessary mission effectiveness of U.S. naval forces.

1.4.3 NCII Functional Capabilities: What Exists and What Is Needed

Tables 1.1 and 1.2 summarize the status of the currently programmed baseline elements of the NCII and the challenges that must be met to give it the capabilities needed for network-centric operations to function as envisioned.

There are many naval, defense agency, and commercial endeavors that can contribute to the development of the NCII. These include the Navy's IT-21 strategy; the Navy/Marine intranet; the Global Command and Control System–Maritime; software radios that can emulate multiple legacy radios and also adaptively select appropriately robust waveforms; the design guidance in the Information Technology Standards Guidance; naval communications and software research at the Office of Naval Research, Naval Research Laboratory, and Space and Naval Warfare Systems Command (SPAWAR); and—in a broader sense—the DOD Global Information Grid as it becomes more specifically defined. In addition, there are valuable DARPA programs that can help advance NCII capabilities in the areas of challenge listed in Table 1.2, including work on information assurance and survivability, dynamic system resource management, agent technology, and data visualization, among others. However, these ongoing developments do not constitute a comprehensive approach to realizing the set of capabilities necessary for an NCII. An integrated overall plan, as well as changes in organizational focus, will be necessary to achieve the NCII.

Key problems include, but are by no means limited to, robust wireless communication networks for tactical environments, content-based system resource management, and scalable information dissemination management. Current conceptualizations of the operational and system architectures seem more suited to situations where requirements can be laid out fully in advance of development rather than to the flexible, iterative process necessary for construction of the

TABLE 1.1 Status of Programmed Baseline NCII

Capability	Assessment
Supporting Resource Base	
Communications and networking	Significantly increased in-theater SATCOM capacity planned, but stated Department of the Navy capacity requirements could be unrealistically low; only limited improvements in tactical communications planned.
Information assurance	Basic network security products being deployed; critical vulnerabilities remain to be considered.
System resource management	Communication channels can be assigned, but priorities cannot be assigned within Internet Protocol (IP) networks. IP advances offer quality-of-service enhancements.
Operational Function	
Collection management	Current capabilities are stovepiped by sensor; limited near-term enhancements are planned.
Information exploitation and integration	Automated extraction of individual targets is accomplished, but much manual work still required for overall battlespace picture.
Information request and dissemination management	Significant improvements in information location and access are promised by information dissemination management capabilities currently being deployed.
Information presentation and decision support	Dynamic two-dimensional, map-based displays of friendly and enemy platforms are in development; overall concept for information needed and means to display it still required.
Execution management	Dynamic mission planning for rapid direction and redirection of forces during operations is limited.

NCII. Sufficient information was not available to the committee to resolve the matter of communications capacity requirements, but it appears that stated future Navy communications requirements could be unrealistically low, even though the available military and commercial satellite communications (SATCOM) capacity is projected to increase significantly. The appropriate division between military and commercial communications will have to be a topic of continuing analysis, planning, and adaptation as the NCII is built and operated.

However the division between military and commercial communications is made, extensive use of commercial communications infrastructure will be inevitable. As pointed out in the Naval Studies Board's TFNF study,[9] this need will

[9]See Footnote 5.

TABLE 1.2 Some Remaining Challenges in Providing NCII Functional Capabilities

Capability	Challenges
Supporting Resource Base	
Communications and networking	Rapid configuration and reconfiguration of networks; flexible wireless networks; multifrequency, electronically steerable antennas.
Information assurance	Intrusion assessment; intrusion tolerant systems; preventing denial of service; hardening of legacy systems.
System resource management	Content-based priority management; dynamic allocation of resources.
Operational Function	
Collection management	Integration across sensors, with intelligent cross-cueing and dynamic tasking.
Information exploitation and integration	Automated integration of disparate information; increased automation of feature extraction from images.
Information request and dissemination management	Profile-based dissemination from large and heterogeneous collections of information sources; automated dissemination management policy.
Information presentation and decision support	Intuitive situational displays; comprehensive suite of necessary decision-support tools.
Execution management	Dynamic replanning; real-time simulation.

be most effectively and economically accommodated by direct use of commercial systems and technology. Such use will require the Navy and Marine Corps to adapt their system design and utilization practices to the demands of the commercial marketplace while ensuring security, priority, and uninterrupted access in times of emergency. Information assurance will be an essential factor in the NCII's evolution and adaptation for network-centric operations.

Finally, it must be noted that efforts to maintain the current distinction between the Joint Planning Network and the Joint Data Network, and likewise to maintain unique protocols for imagery data links, appear not only counterproductive in terms of such factors as interoperability, but also unnecessary in light of developing communications and network technology.

1.4.4 Recommendations Regarding the Design and Construction of the Naval Command and Information Infrastructure

1. The Department of the Navy should develop and enforce a uniform NCII architecture across the strategic, operational, and tactical levels of naval forces.

This means that, for all levels, (a) the same set of functions will apply (e.g., as defined in Figure 1.7),[10] (b) interfaces and standards associated with these functions will be the same, and (c) consistent definitions will be used for the data exchanged between the functions. Architectural concepts more advanced than the simple standards-based architectures currently being considered should be incorporated into the NCII to realize the flexible, rapidly configurable information support envisioned for network-centric operations. Standards should be imposed at a level that does not inhibit innovation in function or implementation; for example, radio standards should specify waveforms and transport protocols—not implementation details—to permit multiple generations of software radios to interoperate.

2. The Department of the Navy should develop a comprehensive and balanced transition plan for realizing the NCII. The functional architecture shown in Figure 1.7 provides a conceptual framework on which to base the transition plan, and the specific recommendations summarized at the end of Chapters 5 and 6 for each of the functional capabilities provide a starting point for the transition to use of the NCII.

3. The NCII should be developed in coordination and collaboration with the other Services, the joint community, and National agencies to promote interoperability and build on each other's efforts. It should also allow for incorporation of coalition capabilities, as appropriate, to missions involving coalition forces. One specific near-term opportunity for coordinating with other Services would be, for example, through participation in the joint expeditionary force experiments sponsored by the Air Force.

4. The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN (RDA)), the CNO, and the CMC should join with the other components of DOD to sponsor a vigorous, continuing R&D program aimed at meeting the challenges of creating an advanced NCII. As part of this effort, the Department of the Navy should give serious attention to the many DARPA and naval research programs that have the potential to meet the challenges.

5. The Department of the Navy should work with the ASD (C3I) and the other Services to make the operational and systems architecture products specified in the C4ISR architecture framework suitable for the flexible and rapidly evolving information support that the NCII must provide.

6. The Department of the Navy should conduct continuing comprehensive analysis of communication capacity requirements and projected availability, and should identify remedial actions if significant shortfalls exist. This analysis should include both long-haul communications and tactical data links, including direct links from in-theater sensors.

[10]The tactical domain will, in addition, have its own unique functions that are particular to warfighting mission areas. These are considered in Chapter 3.

7. To the above recommendations that pertain to all applications of the NCII, including at the tactical level, the committee adds two particular recommendations concerning tactical communications:

a. With few, if any, exceptions, new communications networks for tactical operations should conform strictly to the NCII goal architecture and should use appropriate gateways, firewalls, and encryption devices to ensure high quality of service.

b. Terminals of the JTIDS and common data link families should be modified to use NCII standard protocols.

8. The committee also makes several particular recommendations in the information assurance area:

a. Responsibility for information assurance should be assigned at a high enough level within the Navy Department and with sufficient emphasis to ensure that adequate attention is paid to all aspects of this problem in the design and operation of the NCII.

b. A defense-in-depth strategy should be adopted, based on the premise that security vulnerabilities may always remain in any system components.

c. Advances in security technology should be tracked and aggressively applied in the NCII, including its wireless, SATCOM, and land-based communication components.

d. Procedural and physical security measures should be developed to further reduce the risk where the available technology is not adequate.

e. Naval force information assurance efforts should include preparation and training for operations with impaired NCII functionality, including provisions for redundancy in appropriate places and fallback modes of operation.

f. Research to address future critical NCII information assurance needs should be included as an explicit part of the R&D program that is the subject of recommendation 4 above.

1.5 ADJUSTING THE DEPARTMENT OF THE NAVY ORGANIZATION AND MANAGEMENT

1.5.1 Organizational and Management Needs

Four decision support processes are key to implementing the concept of network-centric naval forces for more effective operations:

1. *Requirements generation:* clearly stating operators' mission needs;
2. *Mission analyses (assessments) and resource allocation:* aligning program and budget resources to meet mission needs;
3. *System engineering, acquisition management, and program execution:* integrating, acquiring, and deploying for interoperability; and

4. *Personnel management:* acquiring personnel and managing careers to meet network-centric needs.

The entire decision-making process for definition, acquisition, and integration of forces to achieve network-centric operations is extremely complex and involves all parts of the Navy Department, as illustrated in Figure 1.8.

The committee reviewed the decision-support processes shown in Figure 1.8 and concluded that better integration was needed among them to attain significantly improved networked capabilities. Modifications to business practices in each of requirements generation; mission analysis and resource allocation; system acquisition and program execution; and personnel management, training, and education—as well as the integrated oversight of the entire complex—are needed to achieve the full benefits of network-centric operations.

The committee found that the information network and cross-platform interoperability are not as well represented in the fleet requirements generation process as are the platforms and weapons themselves. In addition, it found that the current requirements generation process is not sufficiently responsive to the demands imposed by the pace of information technology development to keep deploying naval forces at the leading edge of commercial practices. The committee also found that there is no one organization within the Navy operational community that has the credibility and authority to prepare requirements for the seams among subsystems and components supporting network-centric opera-

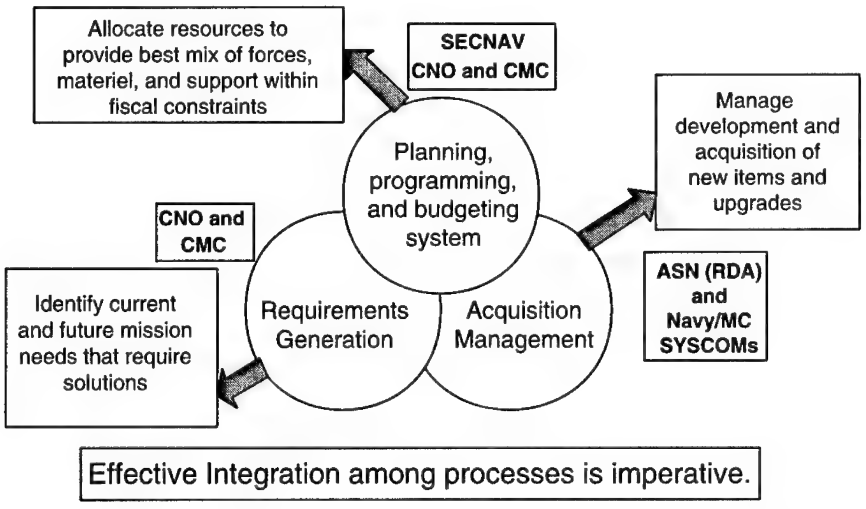

FIGURE 1.8 Major decision-making support processes in the Department of the Navy.

tions. In addition, joint efforts to improve interoperability need expansion. Thus, there is a need to augment the processes by which network-centric operations are internalized to become an integral part of the naval force system.

In the areas of mission analysis and resource allocation, the committee found that the naval forces, taken together, lack good measures of effectiveness (MOEs) and measures of performance (MOPs) for evaluating NCO systems as a whole and the contributions of their subsystems to the larger mission goals. And while the Navy, which has the ultimate responsibility for most naval force system acquisition, has recently taken some steps to enhance the system engineering process within the SYSCOMs (i.e., the NAVSEA 05 organization) and within the ASN (RDA) (i.e., the appointment of the Chief Engineer), there is insufficient system engineering discipline to ensure integration and interoperability of cross-platform and cross-SYSCOM subsystems of any overall NCO system. Possibly most important, in light of the demands of network-centric operations on force evolution and performance integrated across the naval forces and into the joint arena, is the need for more comprehensive review and oversight of the acquisition and program execution of the entire NCO complex of systems within the programming, budgeting, and implementation processes than the current business practices provide. Such review and oversight must include prioritization among the various subsystems.

Finally, some members of the committee believe that, due to the legacy of earlier maritime strategies, the Navy places insufficient emphasis on the power projection mission in the N8 organization and in the program executive office (PEO) structure. The N8 organization reflects submarine warfare, surface warfare, and air warfare, with power projection a part of each office but not the focus of any. Meanwhile, air dominance is well served by the focus of the office of surface warfare, and strategic deterrence by the office of submarine warfare. It appears that power projection lacks a true advocate in N8. The same may be true of sea dominance, although this issue was not examined in as much detail by the committee. In the PEO structure air dominance is the focus of the Program Executive Office for Theater Surface Combatants. At least five PEOs strongly relevant to power projection are primarily product oriented, the products being platforms and weapons in many cases. Therefore, management of end-to-end system designs and acquisitions as such is considered to be problematic. The same may be true for such system designs in other areas, although both the N8 and the PEO structures have been successfully adapted to the need in areas such as ASW and CEC and in the growing theater missile defense (TMD) effort. The ASN (RDA) has recently announced the redesignation of the Program Executive Office for DD-21 as PEO (Surface Strike), assigning it responsibility for NAVSEA Program Manager, PMS 429's Naval Surface Fire Support including the Advanced Land Attack Missile program, as well as the DD-21. This represents a major step in the direction of concentrating attention on power projection systems as a whole, in parallel with the concerns the committee expressed in this

area. The committee's recommendations also pertain to making targeting an integral part of the strike system, to strike warfare from the air, and to the relationship between and coordination of naval surface warfare and air strike warfare. The committee commends the entire power projection area to further scrutiny of the kind that led to this most recent PEO reorganization, in both the PEO and the N8 contexts.

Within the context of this study, other members of the committee addressed and argued against making recommendations on these two issues; they favored what they regarded as more pragmatic recommendations to improve implementation of network-centric operations. Among other things they believe that recommendations on the two issues above will deflect Navy attention from recommendations made in more important network-centric challenge areas—i.e., the recommendations focused on (1) improving integration within and across all decision support processes and (2) developing improved output measures and mission/system component trade-off analyses and assessments. Given these divergent views and the uncertainty they reflect about the true management situation applicable to overall network-centric operations system planning and acquisition, the committee concluded that recommendations to the Navy Department and the CNO would be in order, to review the N8 and the PEO structures and adjust them *if necessary* and *as appropriate* to accommodate end-to-end system designs for NCO subsystems, including especially those relevant to the power projection mission. These recommendations are included with the others that follow.

1.5.2 Recommendations Regarding Department of the Navy Organization and Management

The committee believes that successful network-centric operations will require greater degrees of cooperation, trade-offs, and interaction than currently exist among the stakeholders responsible for the functions involved in NCO integration. It concluded that to best achieve this integration, the Department of the Navy should build on its existing organizations with some changes in emphasis, rather than attempt to totally restructure the department or create a new or additional "stovepipe" for all network-centric responsibilities. The difficulty with even attempting to create a new entity to be responsible for all, or a major portion of, network-centric operations is that such operations span almost the entire range of Navy and Marine Corps activities. Therefore the committee took a pragmatic approach respecting current laws and attempting to minimize organizational disruption.

In arriving at its recommendations, the committee recognized, of course, that internal and external considerations not known to the committee may lead the Navy Department to take other approaches to addressing the committee's findings. The recommended changes represent the committee's best judgments about the best means for the Navy Department to come to grips with the enormous

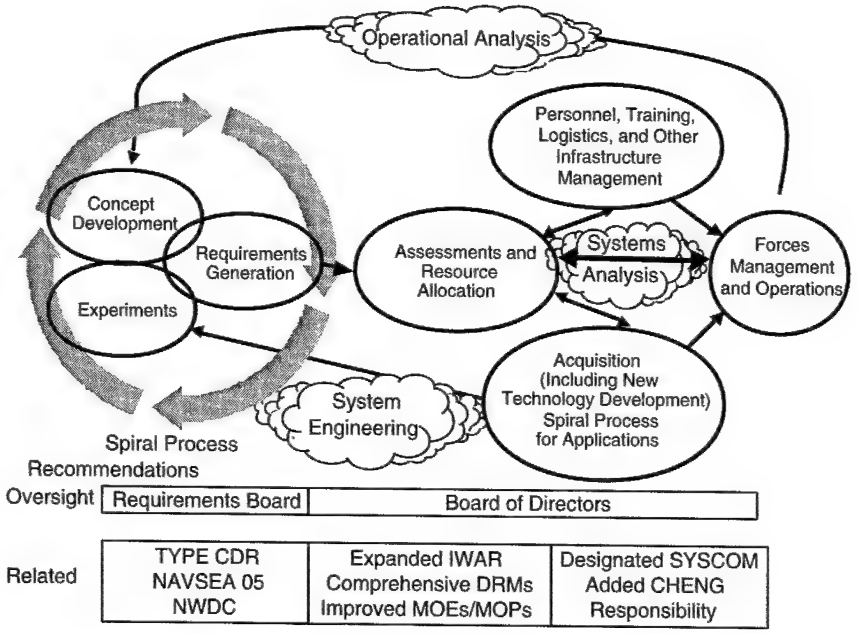

FIGURE 1.9 Functions for effective integration of network-centric operations shown in relation to major recommendations made in this report. CHENG, Chief Engineer of the Navy; DRM, design reference mission; IWAR, integrated warfare architecture; MOE, measure of effectiveness; MOP, measure of performance; NAVSEA, Naval Sea Systems Command; NWDC, Navy Warfare Development Command; SYSCOM, systems command; TYPE CDR, type commander, flag officer responsible for all ships of a certain type in the fleet.

complexities that will attend the evolution of the naval forces into the network-centric operations mode.

Figure 1.9 shows the processes specific to the Department of the Navy that are necessary for effective network-centric operations integration. The committee's major recommendations are indicated below the functions that would be most affected by the specific recommendations.

The major organizational and business process changes and recommendations are summarized in the following paragraphs. They are presented and discussed in full in Chapter 7.

1. The creation of one new position is recommended: a functional type commander,[11] the Commander for Operations Information and Space Command. This new functional type commander should report to only the three fleet commanders, in the same manner as the current platform type commanders report to individual fleet commanders. In addition to assigned operational responsibilities, including management of the fleet portions of the NCII and space assets, this new type commander should be the single point of information support to all the fleets, and should represent the fleet commanders network-centric information operations needs and priorities in the program objective memorandum (POM) and budget processes. He or she would be involved in and support the fleet experimentation program and the recommended spiral development process for network-centric operations. The new type commander would also assume some of the functions now assigned to the Deputy Chief of Naval Operations (DCNO), Space, Information Warfare, Command, and Control (N6) (see Chapter 7).

In arriving at this recommendation, the committee considered various alternate approaches to carrying out the functions summarized above (and described in more detail in Chapter 7). The committee weighed the likely problems and benefits that would attend the creation of the new position. One alternative was leaving the organizational situation as it is now, with a lower-ranking officer functioning with each fleet to deal with its information network matters. This arrangement would not provide adequately for the broad and fundamental nature of the change needed to fully implement network-centric operations in the fleets. The committee also considered a recommendation for creating multiple flag positions for each fleet, but this approach did not appear to resolve the problems of achieving consistency of equipment, planning, and operational techniques in the operational forces throughout the Navy. Only a single individual could achieve that.

After considering the pros and cons of various alternatives, the committee concluded that the time is propitious for making information operations a warfighting mission with a fleet role comparable to that of current type commanders and that the need to achieve assured consistency and interoperability warrants having the functions be the responsibility of a single individual with a high enough rank.

2. A requirements board should be established to deal with operations information and to integrate various competing requirements as presented by the fleets for rapid improvement of complex at-sea operations. The proposed requirements board should be chaired by the VCNO and should have the N6 as the executive director (until the Operations Information and Space Command is established and is assigned that function). The membership of the requirements board should consist of the deputy fleet commanders; the president of the Naval War College;

[11]The flag officer responsible for all ships of a certain type in the fleet.

the DCNO, Plans, Policy, and Operations (N3/5); and the DCNO, Resources, Warfare Requirements, and Assessments (N8). These members should have four broad functions: (a) develop policy and implement strategy for conducting operations based on the NCII, (b) advise the CNO on the strategy and doctrine, personnel, education, training, technology, and resource requirements for moving the Navy from platform-centric to network-centric warfare, (c) establish the linkage to the Navy of the future from this new level of warfare operations, and (d) prioritize emerging network-centric operations requirements based on fleet commanders' recommendations and the results of fleet experimentation.

3. Wherever NCO system needs involving both Navy and Marine Corps forces in joint operations intersect, the Navy and Marine Corps should arrange to coordinate their formulation of requirements.

4. A new board of directors consisting of individuals with the authority to make funding, scheduling, and program adjustments in relevant areas should be established for review, oversight, and prioritization of the acquisition, integrated installation, and program execution portions of network-centric operations. The Undersecretary of the Navy should be the chairman and the VCNO and the Assistant Commandant of the Marine Corps (ACMC) should be members of the proposed board of directors. Other members should be the ASN (RDA) (who should serve as the executive director); the Navy SYSCOMs; the Marine Corps Systems Commander; the DCNO, Plans, Policy, and Operations (N3/5); the DCNO, Resources, Warfare Requirements, and Assessments (N8); the Assistant Chief of Staff (ACOS), Plans, Policy, and Operations; and the ACOS, Programs and Resources of the Marine Corps staff. Requirements sponsors (N2, N4, N6, N85, N86, N87, and N88) should be advisory members to be consulted concerning operational impacts of potential program adjustments. The board's mission should be to provide a focus for network-centric operations and to ensure appropriate integration and interoperability for all acquisition and program execution (including installations in battle groups), for all cross-platform systems, including new subsystems, major subsystem components, and upgrades to existing subsystems and major subsystem components, of the overall system complex for network-centric operations.

5. The Department of the Navy should establish a three-star deputy to the ASN (RDA) for Navy NCO integration to carry out the acquisition and program execution directions of the proposed board of directors. The deputy should be a designated Navy SYSCOM commander and be double-hatted into this role. He or she should oversee all aspects of Navy system interoperability and integration and execution of NCO programs, including the NCII in Navy areas of responsibility. This also includes oversight of the activities of the Navy Chief Engineer and the NAVSEA 05 battle force interoperability engineering function and working with the Commander, Marine Corps System Command, to ensure effective, coordinated program execution in areas where the subsystems of both Services must operate together as part of an overall NCO system.

6. The Department of the Navy should define responsibilities, empower corresponding organizations, and provide adequate resources to (a) establish a comprehensive view of the capabilities and programs necessary to implement the NCII, and (b) see that these capabilities are realized. The assignments of responsibility for the NCII should be consistent with responsibilities for positions established in law and the other naval force organizational changes that are recommended herein. The assigned responsibilities should include interaction with other Services, the joint community, and defense agencies:

— Resource allocation and requirements sponsor: OPNAV N6;

— Operational NCII architecture: Commander, Operations Information and Space Command, with the support of OPNAV N6;

— Policy and standards: Department of the Navy Chief Information Officer;

— System and technical architectures (including enforcement): Navy Department Chief Engineer;[12]

— Acquisition and procurement: program management as designated by the ASN (RDA), and coordination of network-centric operations integration by the designated SYSCOM commander with functions described in 5, above; and

— Operational management of the NCII: Commander, Operations Information and Space Command.

7. Mission analysis and component trade-off evaluations should be strengthened by (a) providing staff and resources for the IWAR development process to enable continuous assessments from requirements generation through programming, budgeting, and execution; (b) developing output-oriented MOEs and MOPs for network-centric operations; and (c) developing a comprehensive set of design reference missions across all mission areas. Resource planning should be adjusted to support the spiral development process, including out-year funding to ensure that it is sustained.

8. The Chief of Naval Operations and the Commandant of the Marine Corps should review how system trade-offs and resource allocation balances are addressed in the Navy/Marine Corps staffs for all naval force missions, and particularly for the power projection mission, with a view toward orienting the process to the overall network-centric operations system concept.

9. Under the Deputy ASN (RDA) for Navy network-centric operations integration, the role of the Navy Chief Engineer should be strengthened to institutionalize the system engineering discipline for integration and interoperability of cross-platform and cross-SYSCOM subsystems and components of the overall network-centric operations system. The Navy Chief Engineer should oversee a system design and engineering cadre drawn from the three Navy SYSCOMs (and the Marine Corps SYSCOM when necessary, appropriate, and agreed to by the

[12]The operational, system, and technical architectures are defined in Chapter 4.

Services) for this purpose. The SYSCOMs should be provided with resources and staff to support this activity.

10. The ASN (RDA) should seek the best means to address the design and engineering of NCO systems, to eliminate as much as possible any distortion of the overall network-centric operations approach through undue emphasis on any single naval force mission or any one platform. In particular, the Navy Department PEO structure should be reviewed and provision made, as is found appropriate and necessary, for management of the acquisition and oversight of mission-oriented, networked major subsystems of the overall NCO systems. In doing this, special attention should be given to end-to-end (surveillance and targeting through effectiveness assessment) fleet-based land-attack (strike and fire support) subsystems for Navy, joint, and coalition missions.

11. The organization of the Navy's N8 office should be reviewed and adjusted as appropriate and necessary to increase emphasis on all aspects of the power projection mission, including strike and countermine warfare, amphibious and airborne assault, fire support, and logistics support of Marine forces from the sea.

12. The Navy and Marine Corps should recommend that J8 in the Joint Staff set up a joint organization for land attack, modeled on the Joint Theater Air and Missile Defense Organization (JTAMDO). Until such an office is set up, the Navy and Marine Corps should participate more actively in the "attack operations" pillar in JTAMDO that is looking at targeting of time-critical targets, such as mobile missile launchers.

Figure 1.10, reproduced from Chapter 7, summarizes the major organizational and business practice recommendations under the three major decision support processes affected most directly by the individual recommendations (including some additional recommendations at a greater level of detail that are included in Chapter 7). As noted on the bottom of Figure 1.10, NCO education and training are needed for all naval personnel.

1.5.3 Personnel Management, Training, and Education

Achieving gains potentially offered by modern technology for enabling force-wide network-centric operations is not likely with current DOD and Department of the Navy personnel management practices. Since information technology work in the military has been changing dramatically, it is not known exactly what skills will be needed for future efforts. It can be projected from the principles involved, however, that competent personnel will be required to address information and knowledge management (extraction, presentation, and application), technical design (architectures, network design) and sustainment (maintenance of connectivity), and applications (for functional users). All future Department of the Navy personnel will need some level of information technology knowledge.

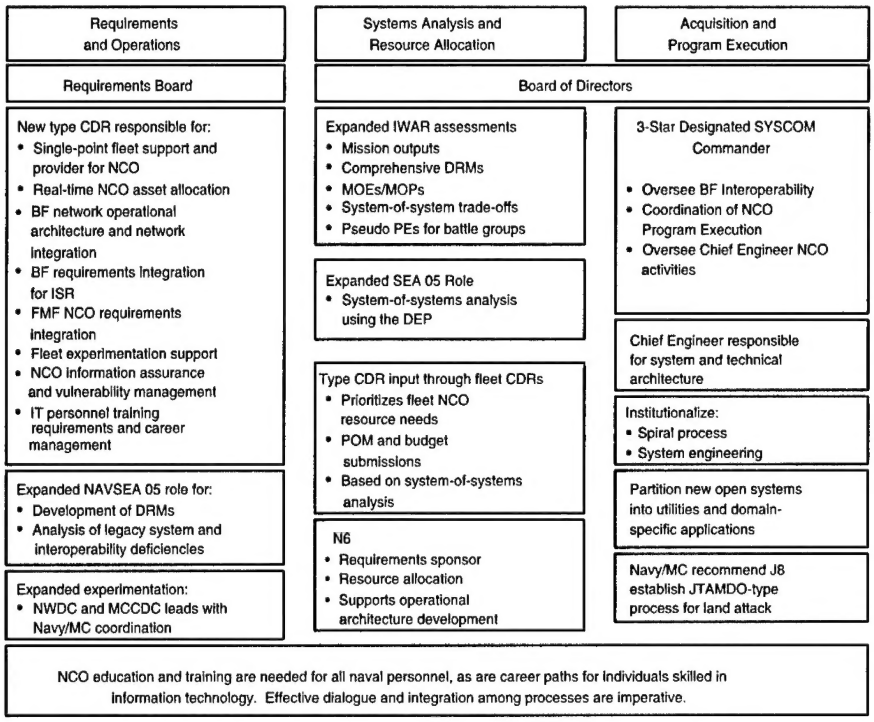

FIGURE 1.10 Key recommendations for managing network-centric operations. BF, battle force; DEP, distributed engineering plant; DRM, design reference mission; FMF, fleet Marine force; ISR, intelligence, surveillance, and reconnaissance; IWAR, integrated warfare architecture; MOE, measure of effectiveness; MOP, measure of performance; PE, program element; POM, program objective memorandum.

Current job skill codes do not provide the detail needed to fully define and manage the emerging workforce structure and skills pertinent to network-centric operations. While some progress is evident (e.g., SPAWAR initiated an analysis of the technical job codes used to identify information technology skills in the military), no systematic effort is under way to examine the job skills required for work involving use of information technology to convert data into knowledge. Within the Department of the Navy, career paths have been established for the newly named Information Technology Specialist rating. However, there are no established related career paths for civilian employees.

The national information technology worker shortage could become a serious problem for the naval forces. Workforce planning to meet information tech-

nology needs must begin now to take advantage of the important opportunity over the next 5 years to realign the workforce as large numbers of current employees retire. In addition, there is a need to analyze the content of the desired information technology work for both the military billet and civilian position structures.

Network-centric operations must be made pervasive in the education of Navy and Marine Corps officers, starting with the U.S. Naval Academy, the U.S. Naval War College, and the U.S. Naval Postgraduate School. Whereas in the past the basic education of naval officers, after leadership, has been focused on platforms—ships, aircraft, submarines—and then on weapons, combat units, and, finally, command, control, and related matters, that education will have to begin by conveying an understanding of the network-centric operations paradigm within which all the other naval force elements are embedded. Beyond that, network-centric operations will have to pervade all the training and education of naval force personnel and Department of the Navy civilian staff.

1.5.4 Recommendations Regarding Personnel Management

The following recommendations pertain specifically to personnel management:

1. The Department of the Navy and the naval forces should institute network-centric operations education and training at all levels across the Navy and the Marine Corps.
2. The Department of the Navy should develop a process for (a) identifying the qualifications for billets critical to network-centric operations (including both domain and infrastructure experts) and (b) identifying training and education needs for those billets. Military and civilian personnel should train together when the information technology learning requirements and facilities are shore-based.
3. The naval forces should develop career paths for both military and civilian personnel to retain and reward those with information technology expertise.
4. The Department of the Navy should analyze and describe the composition and qualities of the current and projected information technology workforce so that more informed decisions can be made about how to distribute specific elements of the work to active-duty or reserve military personnel, civilian employees, and contractor personnel.
5. The Department of the Navy should update information technology job codes to match the work that network-centric operations will require. This update should extend to both military billets and civil service positions.